2003-06

Continuous biometric authentication for authorized aircraft personnel : a proposed design

Carrillo, Cassandra M.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/1011

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

CONTINUOUS BIOMETRIC AUTHENTICATION FOR AUTHORIZED AIRCRAFT PERSONNEL: A PROPOSED DESIGN

by

Cassandra M. Carrillo

June 2003

Thesis Advisor:	Cynthia Irvine
Co-Advisor:	Timothy Levin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Continuous Biometric Authentication for Authorized Aircraft Personnel: A Proposed Design	**5. FUNDING NUMBERS**
6. AUTHOR(S) Cassandra Marie Carrillo	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Federal Aviation Agency	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

Today, there is no way to ensure that the personnel working within the cockpit of an aircraft in flight are authorized to be there. The primary goal of this thesis is to propose a hypothetical design for the use of a non-intrusive mechanism on the flight deck of an aircraft to provide continuous or periodic authentication of authorized aircraft personnel. The mechanism should answer questions such as: "Is the person who is flying the plane actually the person who they say they are?" and "Is the correct person in control of the aircraft throughout the whole flight segment?" We will investigate biometrics as a possible security mechanism.

In this thesis, various biometric methods are examined and their application in the flight deck is shown. Studies that have been conducted on real biometric devices are examined and their results are reported. Also examined are the current practices and procedures that take place in the flight deck, so that the proposed designs can be understood to not interfere with current activities therein.

Two biometric solutions (i.e. proposed designs) to provide continuous or periodic authentication of authorized personnel in the flight deck are introduced. The proposed designs are general and can be used with different types of biometric device(s), and can be extended to include multi-biometrics.

14. SUBJECT TERMS Biometrics, Multi-Biometrics, Multimodal Biometrics, FAA, Biometric Authentication System, Continuous Authentication, Periodic Authentication, Flight Deck Biometrics, Avionics and Biometrics, Computer Security for Aircraft, Hypothetical Biometric Authentication System Design	**15. NUMBER OF PAGES** 113
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

CONTINUOUS BIOMETRIC AUTHENICATION FOR AUTHORIZED AIRCRAFT PERSONNEL: A PROPOSED DESIGN

Cassandra M. Carrillo
Civilian, Naval Postgraduate School
B.S, Computer Science, New Mexico State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2003

Author: Cassandra M. Carrillo

Approved by: Dr. Cynthia E. Irvine
Thesis Advisor

Timothy Levin
Co-Advisor

Dr. Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Today, there is no way to ensure that the personnel working within the cockpit of an aircraft in flight are authorized to be there. The primary goal of this thesis is to propose a hypothetical design for the use of a non-intrusive mechanism on the flight deck of an aircraft to provide continuous or periodic authentication of authorized aircraft personnel. The mechanism should answer questions such as: “Is the person who is flying the plane actually the person who they say they are?” and “Is the correct person in control of the aircraft throughout the whole flight segment?” We will investigate biometrics as a possible security mechanism.

In this thesis, various biometric methods are examined and their application in the flight deck is shown. Studies that have been conducted on real biometric devices are examined and their results are reported. Also examined are the current practices and procedures that take place in the flight deck, so that the proposed designs can be understood to not interfere with current activities therein.

Two biometric solutions (i.e. proposed designs) to provide continuous or periodic authentication of authorized personnel in the flight deck are introduced. The proposed designs are general and can be used with different types of biometric device(s), and can be extended to include multi-biometrics.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Cynthia Irvine for introducing me to this subject, for generating my interest in this area of study, and for helping me become a stronger person academically. Her helpful ideas and suggestions helped me in successfully completing this research. I thank Tim Levin for his meaningful discussions on the subject and his constant support in helping me to get my ideas across. I thank all of the people from the Federal Aviation Administration for funding this research. I would especially like to thank Ernest Lucier and Marshall Potter with the FAA for their support and meaningful answers to my many questions. I am very thankful for the National Science Foundation Scholarship for Service program, which gave me a chance to attend this prestigious institution. I would also like to give a special thanks to the faculty/staff at the Naval Postgraduate School for helping me successfully complete the curriculum; especially Tanya Raven, who gave me her constant support and encouragement before and during my studies at the Naval Postgraduate School. I thank my parents and sister for their constant support throughout my schooling. Lastly, I am grateful for my wonderful husband Marcos who provided me with his constant support, love, and understanding throughout this research.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

As we rush into an increasingly security conscious world, we need ways to pave the road ahead. In the area of avionics mechanisms to provide positive identification of authorized aircraft personnel onboard all aircrafts are needed. Many current security measures have focused on our airports. In contrast, the purpose of this study is to examine security measures related to the inner flight deck area of an aircraft. At this time, there are not adequate security measures set forth inside of the flight deck to provide us with information such as who is flying the plane, who is inside the flight deck, or even if the appropriate persons are in charge of the aircraft for the entire flight. An authentication method is needed to provide this information. The goal of this thesis is to propose a flight deck biometric authentication system designed to provide a positive identification scheme and to provide continuous or periodic authentication of authorized aircraft personnel.

Various biometric techniques suitable for providing continuous or periodic authentication currently exist. This study examines various techniques. It is not possible to cover every biometric technique as limited information has been released about them. Furthermore, this study investigates related issues regarding processing time, computing power, performance measurements, and methods of protecting the biometric data that would be output by a flight deck biometric authentication system.

Using biometrics in the flight deck of an aircraft is a practical solution because biometrics, unlike other forms of identification, personal characteristics provide a positive identification scheme, cannot be lost or stolen, and are a part of us. The last point is what makes biometrics so unique in terms of the physical identification schemes we are used to. We may provide identification to a security guard at work using our employee ID card but that card is not physically a part of us, it is only an object we carry with us. Biometric features are what we are and are always with us. Biometrics is convenient and always available.

Incorporating a flight deck biometric authentication system in commercial aircraft is technically feasible. There are many products on the market to choose from that are relatively easy to use. Since the cost of biometrics is decreasing, it would be reasonably affordable to implement such devices in commercial aircraft.

Two designs are introduced in this study. Design #1 takes advantage of the vast growth and trustworthiness of networking based on secure communication channels. Design #2 takes advantage of trusted PCs onboard the aircraft and the storage capacities of DVD technology. Distributed enrollment facilities are incorporated into both designs to allow the storage of biometric information in reliable decentralized databases. In addition, distributed matching facilities are included in both designs to allocate an external location for biometric template matching purposes and DVD backups. Both designs are expandable to meet the evolution of biometric technology and to incorporate the ideas of others.

Since biometric technology is continuously growing, it will only become better and flight deck authentication schemes will also improve. Neither one of the designs in this study are confined to using a specific method of biometrics. No one method of biometrics is preferred over another for use in commercial aircraft in coordination with either flight deck biometric authentication system designs proposed here. It is hoped that this study may serve as a baseline for implementing biometric authentication in the flight deck and that it may provide the basis for future studies.

I. INTRODUCTION

There have been many world events that have directed our attention toward safety and security. In particular, the tragic events of September 11, 2001 have increased our attention to security in airports as well as in our aircraft. Most of the attention to security has been obvious; such as improved screening of passengers in airports. Does visible security actually aid computer attackers or terrorists who play close attention to the development of such security techniques? Would we feel safer if security were transparent to us or would it be an invasion of privacy? What about implementing security with controlled access to sensitive areas, such as the flight deck of an aircraft? This study will look at biometrics and its use within the flight deck of an aircraft to provide continuous or periodic authentication of authorized personnel while in flight. Two designs, for use on the flight deck, are proposed in this study.

Biometrics refers to the identification of a person based on his or her physiological or behavioral characteristics. Today there are many biometric devices based on characteristics that are unique for everyone. Some of these characteristics include, but are not limited to, fingerprints, hand geometry, and voice. These characteristics can be used to positively identify someone. Many biometric devices are based on the capture and matching of biometric characteristics in order to produce a positive identification. By employing a biometric device or system of devices inside the flight deck, we will be able to tell exactly who is in control of our planes.

This study begins by reviewing several biometric methods and how they evolved into the technologies we now use. This study goes into greater depth on current biometric methods; including the pros and cons of each, how they are used, and influences that may affect the results from a biometric device while in use. A brief summary of where biometrics is already implemented is discussed. Since this study is focused on proposing a design for use within the flight deck, current flight deck procedures are examined.

Some people may question the use of biometrics in the flight deck because biometrics is a relatively new technology. This study takes into consideration the possible vulnerabilities that exist in biometric devices or a system of devices. With every new technology there are vulnerabilities that someone, if given a chance, will take advantage of. It is easy to talk about the vulnerabilities and to take advantage of those vulnerabilities but if we are aware of them, we may be able to design a system that mitigates such weaknesses. Vulnerabilities for the proposed designs are discussed and several ways to alleviate them are suggested.

Every biometric device or system of devices includes the following three processes: enrollment, live presentation, and matching. The time of enrollment is when the user introduces his or her biometric information to the biometric device for the first time. The *enrollment data* is processed to form the *stored biometric template.* Later, during the *live presentation* the user's biometric information is extracted by the biometric device and processed to form the *live biometric template.* Lastly, the *stored biometric template* and the *live biometric template* are compared to each other at the time of matching to provide the *biometric score* or *result*. Each of these processes is discussed in detail including possible faults, which may occur at any time.

Newer biometric methods are emerging daily and this technology is becoming more popular. In this study, the newest biometric system technique, multi-biometrics or multi-modal biometrics is introduced. This technique takes two or more biometric methods and combines them to form a stronger biometric system (in some cases). There are ongoing research projects in this area and this study takes a look at one of these studies and describes how such a system can be successfully implemented. Performance is an important factor when considering the implementation of any biometric device. This study looks at various performance measurements of biometric devices and explains what each measurement means and how it can affect whether the user of the device is accepted or rejected. Some performance measurements are the false acceptance rate and false rejection rate. The false acceptance rate is the rate at which impostors are "falsely" accepted by the system whereas the false rejection rate is the rate at which legitimate users are "falsely" rejected by the system.

Careful examination of current biometric studies gives us an insight on how certain biometric devices perform and what their error rates are. This study explores several of these studies; i.e., how they were conducted, the type of subjects used in the experiments, and the conclusions. These studies indicate that advertised performance measurements from the manufacturers are not always accurate, due to various laboratory or device settings.

Strong security mechanisms, policies, and procedures need to be defined for successful implementation of a biometric device within an aircraft. Several recommendations are given for the various devices that may be used in conjunction with either one of the proposed designs. This study does not recommend a particular biometric method for use in the flight deck but rather makes suggestions regarding which methods may be used and how they can be implemented either by using a single biometric device or a multi-modal biometric system. The two proposed designs are intended for general use and may be implemented with any biometric method that exists today or in the future.

A. PURPOSE OF STUDY

The purpose of this study is to propose a hypothetical design (or several designs) to provide continuous authentication of authorized aircraft personnel as well as guidelines for evaluation of biometric technologies for continuous authentication. This design will include, and is not limited to, the technology of biometrics as an authentication tool. Also considered is the idea of combining biometrics with another type of authentication mechanism such as the use of passwords or smart card technology. By combining what a person knows (e.g. password), what a person has (e.g. smart card), and what a person is (e.g. characteristics that are unique to them) there is a better chance that the system as a whole will yield the correct answer. It may be possible though, to only use two of the three functions to achieve this goal.

By providing a mechanism such as biometrics, we will be able to authenticate authorized personnel in the aircraft with the most up to date and accurate information possible. This information must be stored in a secure area and should not be vulnerable to well known attacks. Since biometric techniques rely on unique human characteristics, it is necessary that this user data be protected.

One challenge with biometrics is how and where the user’s template is stored. This template contains the user’s personal characteristics and the security of this information needs to be stored in a secured database. The storage of this information may also involve privacy issues; these are out of the scope of this study. If this information may be stored in a centralized database, it may become vulnerable to attack and compromise. This study will propose security policies and procedures for protecting this vital information. It is especially important to ensure the privacy of the templates, as users will feel more comfortable about having their personal data stored in the system.

Biometric information must be processed in near real time. Computing power will be a factor in the design. The computing power necessary for particular technologies will differ because of the complexity of the algorithms that are used for matching users to their templates. Complex algorithms should not impact processing time. False/Positive results are a very important factor in a biometric design. Little or no error is needed when authenticating onboard the aircraft. Other important aspects that will be taken into consideration are the failure to enroll rate[1] and the failure to acquire rate[2].

Every biometric system should have general requirements. The UK Biometrics Working Group outlines some general system requirements of all biometric systems [29]. These will form a basis for the design considerations in this study.

- The ability to add and delete users.

In order to ensure that only authorized users are using the system, the people who are responsible for maintaining the system must be able to add users when necessary (i.e. a new employee) and delete users (i.e. a fired employee or one who may have quit the job). If an unauthorized person is able to use the system, that defeats the purpose of this requirement.

[1] Measures the proportion of individuals for whom the system is unable to generate repeatable templates.

[2] Measures the proportion of attempts for which the system is unable to capture or locate an image of sufficient quality.

- Enrollment of the users

The user may use the biometric device for authentication once they have enrolled their digital information into the system. This digital information will be saved as a template (the stored template) that will be compared with the digital image that is scanned at the time of verification (live template). A biometric system can only verify that the individual is who he or she claimed to be during enrollment. With this idea in mind, this proposed system must be able to determine if a person has duplicate enrollments (i.e. a person may have enrolled into a system as someone else and when that legitimate person enrolls, they will have a duplicate enrollment).

- Biometric template, which includes the user's biometric characteristic that is provided to the sensor during both enrollment and live presentation.

This study will look at the accuracy of data collection between all of the biometric devices in question. Data collection is a very important part of the verification and authentication process. The data that is collected must be as accurate as possible. In order for the user to be accepted by the system, their characteristic that is presented to the system must be of sufficient quality to the system.

- Transmission of the captured data.

In the proposed designs, once the data is presented to the system and is matched with the stored template; it has to be sent to the appropriate personnel for monitoring. This is the scenario presented to describe the ideal behavior of the proposed design in this study. The transmission of the captured data must be sent through secure channels and cannot be tampered with or modified in any way. This means that this data cannot be vulnerable to common attacks (e.g. man in the middle attack leading to impersonation or spoofing of identities). This study will present analysis of the appropriate communication channels for biometric data.

- Matching, where the live biometric template from the user's current attempt to access the system is extracted from the received signal, matched with the stored template, and given a "score".

This study will examine the signal processing mechanism and will offer a set of criteria, which will allow the system to rate (e.g. as a metric) the information obtained from the current attempt to access the system compared with the information of the previously stored data in the template (after enrollment has been done). This rating will result in a score based on the comparison mentioned above.

- An authentication policy, which makes the decision to accept or reject the user based upon the system's security criteria and the user's "score".

This study will set forth some security criteria that the system must meet. Along with these criteria and the user's score, as mentioned previously, an authentication policy should be followed in order to make a correct decision to accept or reject the user. If an authentication policy does not currently exist, this study will provide a clear-cut basis for forming one for the flight deck.

- A system security policy covering audit trail information, quality control, system management issues, and level of assurance.

Effective system security policies and procedures are mandatory for a biometric authentication system. Audit trail information should include the time of the event, the event type, and the outcome of the event. System management issues must be taken into consideration because the system under consideration must have strong management properties.

At this current time, there are some serious concerns in regards to the security measures that take place outside of the flight deck area (i.e. weak flight deck doors). This study will explore the security concerns dealing with the inside of the flight deck. It is possible that we may choose to use some type of authentication device outside of the flight deck as well; so much as only authorized personnel are allowed inside of the flight deck.

II. OVERVIEW OF BIOMETRICS

One of the biggest challenges facing society today is confirming the true identity of a person. There are several identification verification schemes that exist today but the most accurate identification schemes are in the area of biometrics. Take the simple example of an ATM card. When a person wishes to use their ATM card, they are required to enter in a personal identification number (PIN) in order to begin their transaction(s). This type of identification verification is given by what that person has (their card) and what that person knows (their PIN). There may be a potential problem to the ATM scheme given above. For instance, the card could be stolen for instance. It would be difficult for the thief to be able to use this ATM card unless s/he knew the PIN. The PIN is vulnerable to theft especially if someone is looking over your shoulder while you are entering your PIN number. This simple example shows that it is practical to use two types of identity verification methods. Biometrics, alone or used with another type of identification verification method, could be an ideal identification verification system used onboard an aircraft.

Some examples of identifying biometric characteristics are fingerprints, hand geometry, retina and iris patterns, facial geometry, and signature and voice recognition. Biometric identification may be preferred over traditional methods (e.g. passwords, smart-cards) because its information is virtually impossible to steal. Although in some cases it may become possible to impersonate a biometric (e.g. replicating legitimate user's fingerprints to fool the fingerprint scanning device).

Two interesting properties of biometric identification are:

1. The person to be identified is required to physically be present at the point of identification and
2. Identification based on biometric techniques does not depend on the user to remember a password or carry a token.

There are two distinct functions for biometric devices:

1. To prove you are who you say you are
2. To prove you are not who you say you are not.

The purpose of the first function is to prevent the use of a single identity by multiple people (e.g. a possible attacker or attackers attempting to take over the plane cannot pass themselves off as a registered pilot). In this case it is important that the biometric device be able to differentiate between a live biometric presented to the scanner (i.e. a real finger) or a spoofed biometric trying to fool the scanner (i.e. a photograph of a legitimate user used to fool a facial scanner). The second function is used to prevent the use of multiple identities by a single person. It would have to be ensured that the biometric system either automatically cross checks the enrolled characteristics for duplicates, or otherwise does not allow a person to register their biometric (i.e. fingerprint) under two different names.

For positive identification, there are also multiple supplemental technologies such as passwords, tokens, and cryptographic keys. An enticing feature of biometric identification is that it could take the place of millions of passwords (e.g. long, hard to remember passwords used to gain access to sensitive information stored on a computer in a large corporation). To provide improved security, biometrics could be used in addition to these alternative technologies and would provide us with the information needed to achieve continuous authentication.

Biometrics has been around for many years. The French anthropologist, Alphonse Bertillon, devised the first widely accepted scientific method of biometric identification in 1870. The Bertillion System, Bertillonage, or anthropometry was not based on fingerprinting but rather relied on a systematic combination of physical measurements. These measurements included measurements of the skull width, foot length, and the length of the left middle finger combined with hair color, eye color, as well as face and profile pictures. By grouping the data any single person could be placed into one of 243 distinct categories. For the next thirty years, Bertillonage was the primary method of biometric identification [3]. Another example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another [3].

Fingerprints are unique to each individual and each individual has their own pattern in their fingerprints. This type of identification has been successfully used by the police to capture criminals and to find missing children. A fingerprint records the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. The traditional method, which is used by police, matches minutiae (details of the fingerprint). Some other approaches are pattern matching, and moiré fringe[3] patterns [3]. There are some verification approaches that can detect if a live finger is presented, but not all of these approaches can provide this type of information. If fingerprint-scanning techniques were to be incorporated into the flight deck to provide continuous authentication, liveness detection or testing would be a requirement for the system.

Fingerprints serve to reveal an individual's true identity and the practice of using fingerprints as a means of identification has been a helpful aid to those who chose to use this type of identification. Fingerprints are unique in the sense that there has not been any type of pattern duplication by two different people. Not even a single instance has been identified or discovered at this time. This uniqueness also applies to identical twins, as well as triplets, quadruplets, and quintuplets. One good thing about fingerprints is that any type of burn (superficial), abrasions, or cuts do not affect the ridge structure, thus the fingerprint pattern is unaffected.

Hand geometry involves analyzing and measuring the shape of the hand. This type of biometric offers a good balance of performance characteristics and is relatively easy to use. The ease of integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric projects. Unlike fingerprints, the human hand isn't unique. It is also known that one could change the geometry of their hands by taking a hammer and smashing it. One drawback for this type of identification is that individual hand features are not descriptive enough for

[3] Moiré fringe is a method used to determine 3D profile information of an object or scene, using interference of light stripes and ultrasonics.

identification. Hand geometry is the granddaddy of the modern biometrics by virtue of a 20-year history of live applications. There have been six different hand-scanning products developed over this span, including some of the most commercially successful biometrics to date [11]. Hand geometry biometric is by far less accurate than other biometric methods.

As an extension to hand geometry analysis, a recent creation by LiveGrip™ analyzes the veins, arteries and fatty tissues of the hand. Sixteen scans are taken and a template of the individual's hand is stored [11]. This method of identification could be costly in terms of storage of templates because sixteen scans are taken, but at the same time, this method does analysis of distinct characteristics of an individual that cannot be changed (i.e. vein geometry, arteries, and fatty tissues of the hand). San Francisco International Airport, the USA's fifth largest airport, has been using hand geometry-based systems to authenticate airport employees for almost 10 years [11]. The U.S. Federal Bureau of Prisons uses hand geometry to track movements of its prisoners, staff and visitors within prisons. Once a person enters the system, they must have their hand scanned. The information is entered into a database and the individual is issued a magnetic swipe card that they carry at all times [11]; this is a good example of keeping track of someone, but one question arises; does this system offer some type of continuous authentication since it is actually tracking an individual? Are they sure that they are tracking the correct person?

A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique uses a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point [21]. This technique may pose a problem if the subject wears glasses or if the subject is concerned with having close contact with the retinal reading device. It is also unknown what types of results are presented in a situation when the user has an eye disease such as cataracts. This technology itself can work well although all users do not accept it.

Retina scan is actually one of the oldest biometrics as 1930's research suggested that the patterns of blood vessels on the back of the human eye were unique to each individual. However, technology has taken more time than the theory to be usable.

EyeDentify, developed the Eyedentification 7.5 personal identification unit, the first retina scan device made for commercial use, in 1984. At this time, they are still the primary company for retinal scan devices though they do use resellers [22].

An iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. This biometric has the potential for higher than average template-matching performance [21]. Ease of use and system integration has not traditionally been strong points with iris scanning devices but as new products emerge, improvements should be expected. The idea of using iris patterns for personal identification was originally proposed in 1936 by ophthalmologist Frank Burch. By the 1980's the idea had appeared in James Bond films, but it still remained science fiction and conjecture. In 1987 two other ophthalmologists, Aran Safir and Leonard Flom, patented this idea, and in 1989 they asked John Daugman (then teaching at Harvard University) to try to create actual algorithms for iris recognition. These algorithms, which Daugman patented in 1994 and are owned by Iridian Technologies, are the basis for all current iris recognition systems and products [21].

In 1999, EyeTicket Corporation[4] introduced JetStream™ for passenger processing including airline check-in and boarding, passport and visa control, as well as EyePass™ for airport and airline employee access control to secure areas. EyeTicket's JetStream and EyePass programs operating at Charlotte Douglas International airport, USA, at Heathrow airport, UK, and elsewhere have accumulated in excess of 400,000 transactions with 100% accuracy, no false identifications, and no security breaches.

Facial recognition analyzes facial characteristics such as overall facial structure, which includes the distance between the eyes, nose, mouth, and jaw edges. This works in conjunction with a digital video camera that captures the image of the face. This biometric has been widely, and perhaps wildly, touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist, or known criminal) but so far has been unproven in high-level usage. It is currently used in verification only systems with a good deal of success. The development stage for facial recognition began in the late 1980s and commercially available systems were made available in the 1990s. While

[4] The leading developer and provider of iris recognition-based travel management systems.

many people first heard about facial recognition after September 11th, 2001, football fans were introduced to it at the Super Bowl several months earlier [21].

Biometric signature verification goes beyond visual signature comparison in its analysis of the way a user signs his/her name. Signing features such as speed, velocity, and pressure are as important as the finished signature static shape. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Every person has a unique signature but that signature is still vulnerable to duplication. If one person tries to "forge" a signature, they will study their victim's signature and practice that style of writing. However, since speed, velocity, and pressure play a role in signature verification, an attacker would need to know these characteristics prior to attempting to forge a biometric signature.

About 10+ years ago, computers were mainly used for accounting needs. Today, computer use is expanding to every corner of the world. Until now, the computer infrastructure was simply not ready for biometrics or signature verification. Digital signature verification is relatively new and has begun its history within the last 1-2 years. In the past, simply looking at two or more samples of a person's signature to see if they matched was signature verification. By performing digital signature verification, matching is done by comparing the movement of how one signs his/her name as mentioned above.

Voice authentication allows the user to use his/her voice as an input device to the system. Voice commands to computers began with applications that were trained by the user to recognize certain words that were spoken such that the user could, for example, speak to a word processor instead of actually typing the words out. Poor quality and ambient noise can affect verification. Certain voice-scan technologies are resistant to imposter attacks to a lesser degree than finger scan systems.

Biometrics has long been used as a form of identification beginning with the early use of fingerprints as described at the beginning of this section. As technology becomes more robust, we will be able to use devices that are more accurate when using biometrics as a form of identification. More recent forms of biometric authentication include facial recognition and iris/retina scanning. Current research is being conducted in the subject of biometric assurance (confidence that a biometric device can achieve the intended level of security).

When deciding on a biometric device for use in an aircraft, we want to include the best level of security possible, within the physical and operational limits inherent to the environment and we want to be very confident that the device will give us the intended level of security as well as accuracy and near real time results. Current metrics for comparing biometric technologies, such as the crossover error rate[5] and the average enrollment time[6], are limited because they lack a standard test bed on which to base their values. Several groups, including the US Department of Defense's Biometrics Management Office, are developing standard testing methodologies [21].

Along with the positive aspects of biometrics as the technology of choice for individual identification and to catch false identification attempts, each method described above also has its own drawbacks. There are various situations that must be taken into consideration when deciding on a feasible method for continuous authentication of authorized aircraft personnel. It is surprising to see that some of these biometric methods have been used for some time now and the immense growth of technology has made it possible to improve upon these methods.

There are a few security measures concerning airplane flight decks that are being requested by pilots to the FAA currently [28]:

1. Replace flight deck doors and walls on all aircraft with strong panels lined with bulletproof Kevlar material.

2. Install video cameras outside flight deck doors, and monitors inside the flight deck, so pilots can see what's going on back in the cabin without opening the door.

3. Take flight deck keys away from flight attendants, so hijackers can't wrest control of them and gain entry to the flight deck.

[5] Generally stated as a percentage, at which the false rejection rate and the false acceptance rate are equal.

[6] Defined as the time in which a biometric feature is saved as a personal reference either de-centrally on a chip card or PC, or centrally in a data base

4. Allow pilots to carry guns that fire rubber bullets, or a subsonic, frangible round, that would not puncture the aircraft's outer shell during pressurized flight.

5. Change flight-crew training so that pilots are discouraged, even prohibited, from leaving the flight deck to resolve passenger or other problems in the back of the plane.

Of these proposed security measures intended for the flight deck of the plane, there is no mention of biometrics or anything intended for the inner flight deck area. These security measures are far more concerned with the exterior of the flight deck, while this particular study is concerned with the inner flight deck, behind the reinforced doors where control of the aircraft takes place. The security measure requests mentioned above all have good reason behind them but as with any type of security measure, they all are vulnerable to some type of penetration or attack. Because these precautions are vulnerable, it is practical to say that if there were also some type of security measures mandated specifically for the interior of the flight deck in addition to the concerns with the exterior of the flight deck, this would make it even more difficult for an attacker to "take over the plane". This security measure inside of the flight deck could be achieved by implementing a biometric device, possibly along with an additional authentication device to achieve continuous authentication.

Biometric technology has been put in place in some markets at this present time and this technology looks very promising. Some vertical markets using biometrics include [16]:

1. Government – driver's licenses, voter cards, etc;
2. Transportation – airport security, boarding passes;
3. Healthcare – patient/employee identity cards;
4. Financial – ATM cards, credit cards (which contain a photo of the holder)
5. Security – personnel access control and identity verifications (which includes time and attendance);
6. Public justice and safety – prison ID's
7. Education – student/teacher identity verification and access control.

Most of us are familiar with or have used many of the types of identification methods mentioned above. These are examples of the simplest types of identification methods that we use everyday (driver's license, employee identity cards). Biometrics is not a new concept, we all have been subject to it in some way or another and some of us actually prefer to provide identification via biometrics. Others may have security concerns when it comes to storing their biological trait information in a central database somewhere or even allowing that information to be contained in a little chip on an ID or credit card. Designers of biometric systems must keep in mind that personal biological trait information is sensitive and must be safeguarded with the appropriate security mechanisms.

If biometric technology were to be brought into the flight deck of a plane, there would be a better sense of security surrounding all of those who use the device (s). It is difficult to estimate the cost of an impending threat so we want to be able to thwart the threat before it becomes reality. Vulnerabilities should be defined and alleviated prior to implementation.

Continuous authentication takes biometrics one step further. Of all of the biometric technologies that are in current use, none of them mention the term "continuous authentication", the authentication process is a one-time event (i.e. placing your palm on a palm reader so that you are allowed to enter a certain area of a building). One major break-through in the world of biometric technology would be to offer a mechanism that would provide continuous authentication for a given amount of time needed (i.e. the duration of a flight).

A. ADVANTAGES AND DISADVANTAGES OF BIOMETRIC TECHNIQUES

No biometric solution will be 100% secure, but when compared to a PIN or a password, biometrics may offer a greater level of security. Biometrics in general holds a set of advantages and disadvantages, as the table below summarizes.

Advantages	Disadvantages
Positive Identification	Public Acceptance
You can’t lose, forget, or share your biometric information.	Legal Issues
A biometric template is unique to the individual for whom it is created	Possible increase in hardware costs to current systems.
Rapid identification/authentication	May require large amounts of storage
Costs, in general, are decreasing	Privacy Concerns

Table 1. General Advantages/Disadvantages of Biometrics

The advantages outweigh the disadvantages primarily because of the first point, biometrics provides positive identification. The ultimate goal is to be able to obtain positive identification without having any doubts. Since one can’t lose, forget, or share their biometric information, then it is known positively that the valuable information cannot be falsified. Although it is very difficult to falsify a biometric trait of an authorized user, biometrics (e.g. a face or fingerprint) are not necessarily kept a secret. For example, our fingerprints are left in a wide variety of places in a given day such as at our homes and in the office (our fingerprints are all over our computer keyboards, mice, and coffee mugs).

Once a person has their biological traits put into a template for later identification/verification, it is known that the template is unique to that one individual. Depending on the biometric method that is implemented, identification / authentication can take place in a matter of seconds or microseconds. This time also depends on the type of system that the administrator is using. Although the idea of digital identification is fairly new, there is a great deal of competition today with similar products, which drives these companies to lower the cost in general.

Public acceptance is the most important issue when implementing a new system or methods by which one abides. If the public does not accept the notion of biometrics, it would be difficult to implement successfully because it would not be used. There is a long list of legal issues that biometrics imposes. Legal issues are out of scope for this study.

Integrating a biometric system into an environment where authentication is necessary is easy if brand new systems were integrated to just do that (i.e. implementing only fingerprint scanners in the flight deck). There may also be existing systems that the integrator may want to upgrade. Hardware costs will definitely increase and that may become a drawback for an agency or enterprise to use biometrics as a means for identification / authentication. The cost of new technology will always become an issue. Storage allocation of biometric templates will also increase and may pose a problem with those who may not comprise sufficient amount of storage at the current time.

Table 2 summarizes the advantages and disadvantages of various current biometric techniques on an individual basis.

Technology	Advantages	Disadvantages
Fingerprint scanning	-Inexpensive -Very secure	-Physical contact to a general scanning device may spread germs.
Hand geometry scanning	-May lead to a better technology (measurements of the vein structure in a hand)	-Not as unique as fingerprints
Retina-based scanning	-Accuracy is assured since the retina remains relatively stable throughout a lifetime.	-May not be generally accepted since the user must come into close contact with the scanning device.
Iris-based scanning	-Very difficult to fool	-Expensive
Facial recognition	-Process can be invisible	-Expensive -Accuracy
Voice authentication	-Widely known to work well over the telephone -Low Cost -May be able to measure stress.	-Background noise or sickness (soar throat) may cause interference -Voice can be easily changed.
Signature verification	-Widely accepted	-Accuracy is difficult to ensure

Table 2. Advantages and Disadvantages of various biometric techniques

As Table 2 indicates, the advantages of fingerprint scanning clearly outweigh the disadvantages. Fingerprint scanning offers a very secure means of identification in an inexpensive way. The only disadvantage is that there is contact with a general scanning device that may spread germs. Simply offering antibacterial cleansing solution before and after the individual scans his/her finger may alleviate this problem. One may also stereotype fingerprinting as a means of identifying criminals although the type of fingerprinting done here is by digital means (e.g. a scanning device rather than traditional ink and paper). Although hand geometry scanning is not as unique as fingerprints, this technology may impose a better means of identification such as vein structure, which is just as unique as a fingerprint. Both retina and iris based scanning techniques are very accurate and difficult to fool. Since the retina remains relatively constant during a lifetime, accuracy can be accomplished with little thought about environmental factors. Retina scanning is considered an exceptionally accurate and invulnerable biometric technology and is established as an effective solution for very high security environments. Retina scanning may not be widely accepted because the individual has to come into close contact with the scanning device and some people may feel uncomfortable with having a laser scanning right at their eyes.

Individuals are familiar with signature and voice verification methods as a means of identification verification on a daily basis. The accuracy of signature verification cannot be ensured. A signature may change depending of various factors such as arthritis, temperature of the hand, or stress levels. This is the same for voice authentication because any type of background noise or sickness (e.g. soar throat) may affect accuracy. Both of these methods are widely accepted but do not provide the type of security necessary in the flight deck of a plane. This premature assumption does not state that voice and signature verification methods cannot be used in conjunction with other methods to provide continuous authentication in the flight deck.

Security, especially in airports, is a major and important issue since September 11 and there has been an interest in integrating biometric technology in airports as well as inside of the flight deck since then. Biometrics will not serve as a replacement technology, but it will serve as an enhancement. Layered with existing access control systems, it may provide an exceptional level of security for both the public and private sectors [30].

B. BIOMETRIC DEVICES: PROPERTIES OF BIOMETRICS

The automatic capturing (i.e. enrollment or authentication) of biometric sample data and comparison (i.e. matching) with previously stored characteristic or normative data requires the following properties of biometric characteristics:

- Invariance: The biometric characteristic should be constant over a long period of time. This would eliminate the need for constant updating of the templates that are stored in the system. For example, the iris is constant throughout a person's lifetime as compared to facial characteristics (which may change due to aging).
- Measurability and Timeliness: The personal characteristic must be able to be automatically compared to an expected norm. The biometric sample should be suitable for capture without waiting time, which is important for continuous authentication and other complications because we want to use a technique which will provide near real-time identification. The flight deck biometric authentication system needs to be able to capture the biometric information from the legitimate user with decreased system result waiting time.
- Singularity: The biometric characteristic should have sufficient unique properties in order to distinguish one person from any other. This is true for all biometric characteristics.
- Reducibility: The captured data should be capable of being reduced to a size that is easy to handle but impossible to duplicate. This property is important especially when we are dealing with communicating the biometric data across secure channels (i.e. from the authenticating device to the controller of the results which may be in a remote area).
- Reliability: The biometric technique should ensure high reliability and integrity. The flight deck biometric authentication system needs to be

reliable because it would be costly to have a system that does not provide consistent results.

- Privacy: The biometric technique should ensure the privacy of the person using the system so that they are convinced that their privacy is not being violated in any way.

All of these properties are important to all biometric characteristics (e.g. iris, retina, fingerprint, and facial characteristics) because we want to be able to provide an accurate way of authenticating authorized personnel in the flight deck.

C. INTRODUCTION TO FACIAL RECOGNITION

Facial recognition systems analyze facial characteristics. This system requires a digital camera or a camcorder to develop a facial image of the user for identification. The facial recognition technique is one of the fastest growing areas in biometric technologies [11]. Facial recognition software measures characteristics such as the distance between facial features, for example, from pupil to pupil, or the dimensions of the features themselves such as the width of the mouth. Some of these devices also perform a "liveness" test to see how your face moves, so that a photo of the user cannot be used [11]. This "liveness" test would be a necessity essential for determining flight deck status.

Facial recognition may be generally accepted by users since it uses a digital camera and we are somewhat accustomed to taking photographs or being in a photographic situation (i.e. taking a picture for an ID card or a driver's license). People are used to identifying others by their facial features (i.e. such as viewing a photograph).

For any biometric system there has to be some user knowledge of the device in the first place. If the user does not know how to use the device, for example, that may lead to higher rejection rates by the system. If the user is comfortable with the system and has been trained to properly use it, then the acceptance rates as well as user- to-system compatibility will increase.

In the case of facial recognition, it is possible to transparently capture facial images of individuals and compare those images to a database of known criminals, for example. There is a concern regarding transparent capturing of facial images of innocent individuals, mainly due to the fact that they are not aware, or haven't agreed to be part of the "virtual criminal lineup". Privacy issues related to this type of situation will not be addressed in this study.

1. How Facial Recognition Works

There are about 80 nodal points on a human face. Some nodal points that are measured by facial recognition software are the following:

- Width of nose
- Depth of eye sockets
- Width of cheekbones
- Jaw line
- Chin

These nodal points are measured to create a numerical code that represents the face in a database [4]. Facial recognition methods may vary, but they generally involve a series of steps that serve to capture, analyze, and compare your face to a database of stored templates. There are several facial recognition tools currently out in the market, one such example is called the FaceIT® system[7]. Listed below is the basic process that is used by this system to capture and compare facial images [4]:

- Detection: When the system is attached to a video surveillance system, the recognition software searches the field of view of a video camera for faces. If there is a face in the view, it is detected within a fraction of a second. In the case of identification in the flight deck of a plane, for example, the camera would be positioned where there would generally be a face in full view.

[7] http://www.wei-usa.com/FaceIt.htm

- Alignment: Once a face is detected, the system determines the heads position, size, and pose. A face needs to be turned at least 35 degrees toward the camera for the system to be able to register it.
- Normalization: The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose.
- Representation: The system translates the facial data into a unique code.
- Matching: the newly acquired facial data is compared to the stored data and (ideally) linked to at least one stored facial representation.

Raw data, such as an actual photograph, of users' faces is not stored in the system. Instead, the software stores the images as unique codes that only the computer can comprehend. Because unique codes are stored in the system, it is difficult for an attacker to spoof the biometric information. Also, an attacker would not have the ability to extract an actual photograph of the legitimate users of the system. The attacker would only be able to extract numerical codes.

The heart of the FaceIt® facial recognition system is the Local Feature Analysis (LFA) algorithm. This is the mathematical technique the system uses to encode faces. The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of faceprints stored in a database. The system can match multiple faceprints at a rate of 60 million per minute from memory or 15 million per minute from hard disk. As comparisons are made, the system assigns a value to the comparison using a scale of one to 10. If a score is above a predetermined threshold, a match is declared.

2. Facial Recognition: User Influences

Every person carries unique characteristics in their facial features. Factors such as the distance between the eyes and the shape of the nose play an important role in distinguishing a person digitally. The one factor that separates facial recognition from other biometric technologies is the fact that the face is a changeable surface, displaying a variety of expressions, as well as being an active 3D object whose image varies with viewing angle, pose, illumination, accoutrements, and age [29].

It has been shown that for facial images taken at least one year apart; even the best current algorithms have error rates of 43% - 50% [29]. This error rate range would not be acceptable if it were employed in the flight deck for continuous authentication. The fact that this error rate range corresponds to a one-time authentication step, it is quite possible that this rate may fall well below 10% when it is applied to continuous authentication. It is also possible that there may even be a better algorithm for use in this situation.

When considering facial recognition as a form of identification, there are some user-based influences that must be taken into consideration. Some user-based influences are [29]:

- Beards or moustaches
- Baldness
- Height
- Skin tone

Beards and moustaches play a major role in acceptance rates. It is possible that an appearance or disappearance of facial hair may have an effect on rejection rates for the male population. The same argument can be made about the influence of baldness. A slowly receding hairline may cause rejection by the system, if in fact; the forehead size is a part of the user template. For example, a receding hairline may cause the forehead to appear larger and that person may have to re-enroll their information into the system once again and the same would be true for a man who usually wears a beard or moustache and decides to shave it off completely.

The height of a person may also play a crucial role because the very tall, very short or those in wheelchairs may have difficulty positioning themselves correctly [29]. I feel that the height factor will have little effect in the flight deck of a plane because authorized personnel are usually seated during flight.

Skin tone may also affect whether the user is accepted or rejected by the system as well. For example, there may be a person whose skin pigment does not register very well with the system and are forced to rejection most of the time. The system should be able to adapt to different skin tones and lighting situations.

The users' behavior may also have an influence on the systems acceptance or rejection rates. Some user behavioral activities that may affect the outcome from the system are [29]:

- Facial expression
- Movement or lack of movement
- Head position
- Distance from camera

Facial expressions can indeed affect the system outcome. For example, if a user initially enrolled into the system with a serious look, they should identify themselves to the camera the same way every time (if at all possible). One should not do things such as widening/squinting the eyes or wrinkling up their nose because it is likely that this type of activity will cause a rejection from the system.

Movement or lack of movement may also cause a rejection from the biometric system. If the user is moving too much, an accurate result may not be possible. The same holds true if the user has lack of movement or if the user has their head tilted to one side. Usually the normalization algorithm used for facial recognition would adjust for activities such as these. Lack of movement may also imply that an intruder is showing a photograph of the legitimate user to the facial scanning device. For this reason, it is important that the system is capable of performing "liveness" tests.

In the process of facial recognition, the user may be required to stand or sit a certain distance from the camera in order to achieve desired results. If the user is standing or sitting too far or too close to the camera, then the results may be inaccurate and cause a rejection from the system.

User appearance is another issue that must be taken into consideration. Some user appearance factors are [29]:

- Clothing
- Cosmetics and Cosmetic surgery
- Glasses or sunglasses
- Hairstyle or hair color

Some clothing influences may be hats, earrings, or scarves. Cosmetics whether it is caused by user application or surgical procedure may have an effect on acceptance or rejection from the system. Glasses or sunglasses may also affect the result from the system. It is suggested that if the user initially used glasses while enrolling in the system then they must always use those glasses when identifying themselves to the device.

Hairstyles and/or hair color may also affect the users' acceptance or rejection rate. Since hairstyles probably change faster than hair color, it is suggested that the system adapt to these changes or to completely ignore these changes and pay attention to other important attributes of the face. It would become very costly if the users had to re-enroll themselves every time they made a change to their appearance.

In order to be able to implement an effective system, the user influences described here must be taken into consideration. If this type of system is implemented in the flight deck of a plane, some of these influences may be disregarded.

3. Facial Recognition: Environmental Influences

In addition to user influences, there are also some environmental influences that must be considered. Environmental influences are based on general background, lighting, and weather conditions. These influences are [29]:

- Background, clutter
- Other faces
- Lighting or reflections

- Rain or snow

Background scenery or clutter around the camera may cause problems when a user is trying to authenticate to the system. If there are other faces that are obstructing or confusing the camera or a faint reflection of another face in the background will have an effect on the acceptance or rejection rates of the system. Lighting and weather conditions such as rain or snow (causing redness in the face) also have an effect on system outcome. By identifying these environmental influences there is a better understanding of what we need to pay attention to if facial recognition is integrated into the proposed designs of this study.

Data quality is the key to achieving satisfactory operational performance of the biometric system. The environment under which enrollment or authentication is taking place will affect the quality of the enrollment or authentication/identification function performed by the system. Since this system will be used by a limited number of people (i.e. rather than by millions of patrons in the airport) it is easier to define the environment that the device will be used in and it makes it easier to determine whether the device is being used the way that it is meant to be used.

4. Methods of Facial Recognition

The four primary methods employed by facial scan vendors to identify and verify subjects include eigenfaces, feature analysis, neural network, and automatic face processing. Some types of facial scan technology are more suitable than others for applications such as forensics, network access, and surveillance. The process flow of facial scan technology, as with other biometric techniques, contains 4 steps [17, 31]:

- Sample Capture
- Feature Extraction and storage
- Live and stored template comparison prior to matching
- Matching of the live and stored templates to produce a matching score

A system that is based on using local feature analysis uses a camera and computer to identify a person and analyzes pixels that make up the face image.

A flight deck biometric authentication system using facial recognition should be capable of performing liveness tests and a system based on local feature analysis will be able to perform liveness tests. In order to be sure that the eyes, nose, and mouth belong to a living being and not a mannequin, the program looks for eye blinks or other tell tale facial movements [1].

The Eigenface method examines the face as a whole and is one of the most popular face recognition methods in use today [31]. With a database of headshots on hand, the system compares the face being identified to the composite. The composite is the actual template of the image that is initially stored in the system at the time of enrollment and the target is the live template that is captured at the time of authentication. An algorithm measures how much the target face differs from the composite and generates a 128-digit personal identification number based on the deviation. If the Eigenface method is used, a training set that contains enough number of face examples is needed. The purpose of the training set is to have a number of various templates of the same person. These various templates are expected to cover various conditions such as different head poses, lighting conditions, or facial expressions [31].

Though overall not as robust as eigenfaces, feature analysis, or neural network, automatic face processing may be more effective in dimly lit, frontal image capture situations [31]. In neural network mapping, the enrollment and verification data are compared and there is a vote on whether there is a match between the two. Neural networks employ an algorithm to determine the similarity of the unique global features of live verses enrolled faces. This method, theoretically, leads to an increased ability to identify faces in difficult conditions [31].

D. INTRODUCTION TO IRIS RECOGNITION

An iris-based biometric identification scheme involves analyzing features that are found in the colored ring of tissue that surrounds the pupil. Complex iris patterns can contain many distinctive features such as ridges, crypts, rings, and freckles [7]. Iris scanning uses a fairly conventional camera and requires no close contact between the subject and the reader. Compared to the close contact between the subject and the reader required by some other biometric identification systems such as retina scanning, the subject may feel more comfortable using this type of device. The iris is unique from person to person because there are so many different patterns that surround the pupil. The iris is said to be more unique than a fingerprint. It is possible that the iris-scanning device can successfully read the patterns in the iris even when the subject has a pair of glasses on and this idea has been demonstrated to work in an actual system [31]. This recognition ability would be valuable in the flight deck of an aircraft because it is not known whether the person being authenticated is wearing glasses or not.

1. How Iris Recognition Works

The iris-scanning procedure is simple and painless. All the subject needs to do is to stand at least a foot away from the camera and look into the scanning device. The camera then scans the iris into a pattern that is digitized [11]. The scanned digitized pattern is then compared to a previously recorded pattern. These stored patterns are also called templates, the same idea that is used with other biometric techniques such as fingerprint scanning and facial recognition.

The iris is protected from the environment and is stable over time. The iris would be difficult to duplicate, in order to spoof an authorized user in the system; an attacker would actually need the authorized user’s eyeball, which is highly unlikely to happen under normal circumstances. Furthermore, if the flight deck biometric authentication system consisted of an iris recognition system, liveness testing is possible. The iris-scan systems test for a live eye by checking for the normal continuous fluctuation in pupil size [30].

In order to capture the rich details of iris patterns, an imaging system should resolve a minimum of 70 pixels in iris radius. In field trials to date, a resolved iris radius of 100 to 140 pixels is more typical [30, 31]. There are many advanced algorithms that are used to aid the scanning device in actually locating the iris by distinguishing it from the pupil.

Iris recognition technology converts the visible characteristics of the iris into a 512-byte code, which is a template stored for future verification attempts. Iris-scan technology is primarily deployed in high-security physical access implementations [31], which makes it an ideal candidate to employ in the flight deck. Iris scanning is more accurate than that of fingerprint scanning [30, 31]. Since the user may have to look at the camera for iris scanning for up to 15 seconds, it is not known if this technology can be performed continuously, but it may be performed periodically. Periodic scanning of the iris may be sufficient to achieve close to continuous authentication.

Since iris-scanning technologies are harmless to the eye, there should be no concerns about long-term effects. The only thing that one should be concerned about is having consistent lighting in the area in which the iris-scanning device is located. Poor lighting may have an effect on the scanner's results such as the case with facial recognition.

Iris scanning contains both user and environmental influences. Some user influences are [29]:

- Eyelashes: Eyelashes may have an impact on how accurate the scanning results are because a user may have long eyelashes that may obstruct or confuse the scanner.
- Iris color intensity may also affect the outcome of the scan if an appropriate pattern is not possible due to the color of the iris.
- Height of the user: A very tall or very short person may have trouble positioning themselves to the scanning device for adequate results. However, the user may be seated during scanning and the scanning device may be placed in a universally reachable area.
- User movement: The user has to be able to stay still in order to get an adequate reading.

- User distance from the camera: If the user is too far from the camera then accurate results cannot be obtained.
- Colored or tinted contact lenses may have an effect on user acceptance.
- Glasses or sunglasses may also affect the outcome of the scan. However, some current iris scanning devices are able to give accurate results if the user is wearing clear eyeglasses rather than medium or dark tinted sunglasses.

2. Iris Recognition: Environmental Influences

There are only a few environmental factors for iris scanning techniques:

- Lighting level may have an effect on the iris scanning device outcome. If the lighting level is too dark, an accurate picture of the iris may not be possible and the iris pattern that the device is seeking may not be fairly visible for comparison. On the other hand, if the lighting level is too light, an accurate picture may still be possible but it is not known whether a usable iris pattern can be accessed from the picture taken. Since the user is able to use an iris-scanning device from as far as 3 feet away, the lighting level of the room plays a significant factor on how accurate the scan is.
- Obstructions in the eye will play a significant role on how accurate the scan is taken. For example, if there is a speck of dust in the eye or an eyelash inside of the eye then the iris pattern may not be obtained by the device.

The cleanliness of the lens of the scanning device plays a significant role in obtaining accurate results so the camera lens must be kept clean at all times thus free of any dirt or dust particles, smears, or scratches. Of the influences that are mentioned, none of them pose a serious threat to the scanning device but they must be taken into consideration because they are just little mistakes that the user or administrator of the device may not think will affect the device or the output from the scanning procedure.

E. INTRODUCTION TO RETINA RECOGNITION

Retina and iris scanning are similar because they are both focused on the eye of the user but they are very different from each other because of what these biometric methods use as a basis for their measurements. A retina scanning system records elements of the blood vessel patterns of the retina on the inside rear portion of the eyeball. A camera is used, analogous to iris scanning, to acquire the image in order to map a distinct pattern that is used in comparison to existing template information for the legitimate user. The retina exhibits the characteristic that the blood vessel patterns remain stable throughout a person's lifetime.

With retina scanning, the user must look into a receptacle and focus on a given point. This technique requires that the user have close physical contact with the device, which may or may not be acceptable to some users. Retina scanning is not convenient for those who wear glasses or those who have concerns about having close physical contact with the device. Since a low intensity light is used to record the blood vessel pattern of the retina, it is not known if there are any long-term effects by using this technique for long periods of time.

The retinal image is difficult to capture and during enrollment the user must focus on a point while holding very still so the camera can perform the capture properly. The only thing that is actually determined is the pattern of the blood vessels, but since this pattern is unique in each person, identification can be precise.

1. Retinal Recognition: How It Works

Retina scanning maps the capillary pattern of the retina, a thin nerve in the back of the eye. The subject must be within a half-inch from the device and is required to keep his or her head and eye motionless as they focus on a small rotation point of green light. Infrared light is used because blood vessels on the retina absorb this light faster than the surrounding eye tissue. A video camera captures the retinal pattern and translates it into data that is 35 bytes in size.

For recognizing the patterns, about 400 unique points on the blood vessels are recorded [30, 31]. For recognizing patterns, the previously enrolled pattern (stored template) is compared with against the live blood vessel pattern (live template) of the individual. As with fingerprints, each individual possesses a unique blood vessel pattern in his or her retina. The information contained in the unique blood vessel patterns in the retina would be difficult to spoof because an attacker cannot easily fake these patters either by using fake eyes, a photograph, or a video.

2. Retinal Recognition: User Influences

The user-based influences for retina scanning are almost similar to the user based influences for iris scanning with little differences. Some user-based influences are [29]:

- User height: As explained previously, a user's height may have an affect on how well they are able to reach or use the scanning device. This problem may be alleviated because some scanning devices are able to move up and down to fit the users' height perfectly.
- User movement: If the user has too much eye movement, especially when using retina scanning, it will have an effect on the reliability of the scan.

F. INTRODUCTION TO FINGERPRINT RECOGNITION

Every person possesses unique fingerprints from any other individual. As with other biometric methods, fingerprint identification is based on two basic premises:

- Invariance: The basic characteristics of the fingerprint do not change with time. However, there are instances where a fingerprint reader may not accept a legitimate user because of a cut on the finger or dry skin.
- Singularity: The fingerprint is unique to each individual and no two people have the same pattern of fingerprints.

Fingerprint-based identification has been used for a long time and is routinely used in forensic laboratories and identification units all around the world. Fingerprint evidence has also been accepted in courts of law for nearly a century [21]. The population as a whole is familiar with fingerprint identification methods and this familiarity makes this technique have a high user acceptance rate. In my own experience, I had to use a fingerprint scanner while applying for my California Driver License and the device was not hard to use and the process was pretty rapid. The only step that I took though was enrolling into the system and I didn't have to go through any matching process. The scanning device that I used to get my drivers license was an optical scanner. As I looked at the monitor to see my resulting fingerprint image I noticed how clear the image was.

Fingerprint patterns can be represented by a large number of features [31] including the overall ridge flow pattern, ridge, frequency, location and position of singular points. It would probably be difficult to guess the digital representation of a fingerprint pattern without having the actual finger present.

1. How Fingerprint Recognition Works

A fingerprint-scanning device is pretty easy to use. The user must place his or her finger on the device and certain characteristics of the fingerprint image are extracted into templates known as minutiae. The characteristics of each finger are different from each other.

Recall that finger-scanning systems only store data about specific points of the fingerprint. The only way an attacker would be able to spoof a user to a finger scanning system is by having a legitimate user present his or her finger to the scanning device or to somehow obtain an image of a legitimate user's fingerprint. If the flight deck biometric authentication system includes fingerprint-scanning device, liveness testing must be employed. One way to employ liveness testing in fingerprint scanning is to have the device equipped with a "heartbeat checking" mechanism which would measure whether a heart beat or pulse is present while the user is touching the device. This would require the user to hold his or her finger on the scanning device a little bit longer than usual.

As with other biometric methods, general fingerprint matching process involves three phases:

- The acquisition phase or enrollment is where the fingerprint is scanned using a fingerprint sensor. Many sensors are available that capture a fingerprint based on the optical, capacitive, pressure, thermal, or ultrasound domain. The capturing of the image is made easier because the sensors only require a simple touch of a finger.
- The live presentation phase is when the user shows his/her biometric information to the biometric device.
- During the matching phase, the features of the scanned fingerprint (live template) are compared to the stored template in the database

Since traditional methods of fingerprinting (i.e. fingerprint capturing using ink and paper) are not used that often in fingerprint recognition technology, we are able to capture more details of that fingerprint. In addition, the newer methods of fingerprint recognition are more hygienic and less intrusive. In order for the system to offer accurate results the user has to be willing to use it correctly and they have to be willing to fully understand how the system works. For example, the user will have to know how long they would have to press their finger on the reader in order to obtain accurate results.

2. Fingerprint Recognition: User Influences

Fingerprint recognition methods contain influences that may affect the outcome of the authentication process of the device. Some influences are [29]:

- Fingernail growth may have an effect on how firmly the user is able to place his/her finger on the scanning device. This may result in inaccurate results from the device or the user may be rejected altogether by the system. This influence also extends itself to the use of artificial nails that the user may apply to real fingernails.
- Fingerprint fineness may also have an effect on how the device is able to pick up details of the fingerprint. This depends on how well the depth and the spacing of ridges are on the users fingers. This influence is not

controllable by the user so proper enrollment from the beginning needs to be done as well as proper placement of the finger on the scanning device at the time of authentication. There may be fingerprint-scanning devices that alleviate this influence by offering a sensitive "touching area" for the user.

- The condition of the fingerprint may have an effect on the outcome of the device because the user may have dry, cracked, or damp fingers. If the user has dry, cracked, or damp fingers at the time of enrollment or at the time of authentication the scanning device may not be sensitive enough to compensate for these characteristics. Another influence that falls into this category is scars and/or scratches on the fingertips of the user. Scars and scratches, depending on their location, may cover up some important characteristics of the fingerprint that the scanning device is looking for to extract. On the other hand, it may be possible for the scanning device to simply use the scar on the fingertip as a part of the characteristic extracted.

- Temperature of the user's finger or hand. The temperature of the user's finger may cause inaccurate results from scanning device. I have personally spoken with people who have told me that their fingerprint-scanning device continuously rejects them usually in the morning because their fingertips were too cold. This may also have an effect on the device, if in fact; the device does liveness tests based on temperature of the finger rather than on a pulse on the fingertip.

3. Fingerprint Recognition: Techniques

The techniques used to gather fingerprint information has changed greatly over the years. Some sophisticated fingerprint scanning methods have emerged since the beginnings of this method of identification. Some sophisticated methods currently available are [30]:

- Optical sensors with CCD or CMOS cameras.

The finger is placed or pushed on a plate and is illuminated by a LED light source. Through a prism and a system of lenses, the image is projected on a camera. Frame grabber techniques are used and the image is stored and ready for analysis.

- Ultrasonic sensors.

By using ultrasonic sensors, a scan of the fingerprint with a resolution of about 500 dots per inch is possible. This technique may be able to offer templates, which are full of useful detail of fingerprint information.

- Electronic field sensors.

This technique creates an electric field with which an array of pixels can measure variations in the electric field that are caused by the ridges and valleys in the fingerprint.

- Capacitive sensors.

This technique is similar to electronic field sensors except that when the finger is placed on the sensor, an array of pixels measures the variation in capacity between the valleys and the ridges of the fingerprint.

- Temperature sensors.

This technique makes a distinction between the temperature of the ridges and the temperature of the valleys on the fingerprint. A temperature scan can be taken by simply swiping the finger over the sensor.

Although these techniques seem very advanced and accurate, it is still possible that a desperate attacker may attempt to spoof a legitimate user by creating fake fingers. Fake fingers can be made both by the cooperation of the legitimate user (i.e. for testing methods) or without the cooperation of the legitimate user by lifting a fingerprint off of a keyboard or coffee mug. Those traces of fingerprints are known as *latent fingerprints.* Tsutomu Matsumoto, a Japanese cryptographer, has discovered a means to fool many of the commercial fingerprint scanners available using common ingredients.

One of Matsumoto's more interesting experiments involves latent fingerprints. He takes a fingerprint left on a piece of glass, enhances it with a cyanoacrylate adhesive, and then

> photographs it with a digital camera. Using PhotoShop, he improves the contrast and prints the fingerprint onto a transparency sheet. Then, he takes a photo-sensitive printed-circuit board (PCB) and uses the fingerprint transparency to etch the fingerprint into the copper, making it three-dimensional. (You can find photo-sensitive PCBs, along with instructions for use, in most electronics hobby shops.) Finally, he makes a gelatin finger using the print on the PCB. This fools fingerprint detectors about 80% of the time [27].

As mentioned before, the success of a biometric device lies in the acceptance of that device by the users. If the device is easy to use and does not take too much user time, then most likely it will be accepted and used correctly. On the other hand, if it is difficult to use or takes too much time from the user, the success of the device will be greatly reduced. For example, in the software industry users choose to use the applications that are the easiest to use and that provide them with the features that they expect. That factor alone may determine the popularity and success of the application (i.e. Microsoft Word in Windows vs. *vi* in UNIX).

G. INTRODUCTION TO VOICE AUTHENTICATION

Everyone is familiar with voice communication and feels comfortable with it. We are used to this identification process in our everyday lives, for example, it is easy for us to recognize a voice from long ago which is analogous to the voice authentication system being able to recognize and identify a voice of a legitimate user at almost any given time. That is what highlights the notion of using an individual's voice to uniquely identify who they say they are. Since the pilots and/or copilots already speak in the flight deck, voice authentication would make an excellent choice for implementation in the flight deck because the pilots may not have to perform extra activities in order to authenticate.

Voice authentication is not based on voice/word recognition but rather is based on voiceprints. Voice/word recognition is where complex technology transforms voice into text. This type of technology transcribes spoken words into typed text for use in, for example, a word processing application. Voice command systems that utilize word recognition are already being implemented in automobiles for use with the global positioning system (GPS) for rapid road directions. Voice/word recognition technology merely translates what a user is saying as opposed to voice authentication, which verifies the vocal characteristics of the individual.

Voiceprints are created based on the highs and lows that are specific to the way an individual speaks. Voice authentication is probably the easiest of all biometric technologies to implement but at the same time is also potentially the least reliable because the voice is so easy to alter, even by a legitimate user. For this reason, if voice authentication were to be employed in the flight deck it would have to be accompanied by an additional form of biometric or other authentication mechanism.

It is said that voice authentication is not well developed, partly due to the fact that background noise affects its performance [30]. It is then questionable if this is the case in the flight deck: "Is it so noisy in the aircraft flight deck that it would not be feasible to employ voice authentication?"

1. Voice Authentication: How It Works

Voice authentication technology utilizes the distinctive aspects of the voice to verify the identity of individuals. The pitch, tone, frequency, and volume of an individual's voice can uniquely identify him or her. The downside of voice-based authentication systems is that the voice is one biometric characteristic that can be easily duplicated (i.e. a tape recording of a legitimate user). This method may be used to spoof a system that uses voice authentication by an attacker who may be able to gain a recording of the legitimate user's voice. The good thing is that the authentication process may involve speaking a pass phrase, sequence of numbers, or a password that may make it more difficult for an attacker to be able to record the correct parameters. The pass phrase is something that the authorized user knows, thus this adds an extra layer of security.

During enrollment and subsequent identification processes voice authentication systems make use of the features of the voice. Voice authentication can be easily implemented since most computer systems already have a microphone readily available.

2. Voice Authentication: User Influences

Although voice authentication appears to be an easy authentication method in both how it is implemented and how it is used, there are some user influences that must be addressed [29]:

- Colds. If the user has a cold which affects his or her voice that will have an effect on the acceptance of the voice-scanning device. Any major difference in the sound of the voice may cause the voice-scanning device to react in a negative way, causing the system to reject the user.
- Expression and volume. If a person is trying to speak with expressions on their face (i.e. smiling at the same time) their voice will sound different. The user of the device must also be able to speak loudly and clearly in order to obtain accurate results.
- Misspoken or misread prompted phrases. If the user is required to authenticate by speaking a prompted phrase and they mispronounce the phrase, they will be rejected by the system.
- Previous user activity may have an impact on the outcome of the voice-scanning device. For example, if the user is out of breath and is unable to speak well.
- Background noises will interfere with the user who is trying to authenticate to the device. The environment in which the user is authenticating to the device must be free of any major background noise.

H. BIOMETRICS VULNERABILITIES

Biometrics provides the means to present personal credentials that are unique. Many other systems rely on passwords or tokens as a means of security measures but when it comes to securing the flight deck, this does not suffice. What would cause the flight deck biometric authentication system to be vulnerable to attack? A biometric system as a whole is only as strong as its weakest link, which may not even include the actual biometric information being introduced to the system but rather, the actual system and/or storage of the biometric data collected from that system.

There are several ways that a biometric system and biometric data may be compromised and some will be mentioned here. *System circumvention* is defeating the way in which is system is meant to be used. An example of system circumvention would be an attacker gaining access to the flight deck biometric authentication system and installing a backdoor thus gaining elevated privileges or total control. Since system circumvention would most likely take place remotely, it would be difficult to catch such an attacker without careful analysis of the attack. If an attacker were able to install a backdoor into one of the systems, either the flight deck biometric authentication system or the system that stores the biometric data, they would be able to launch various other types of attacks. For example, if an attacker has access to a system that caches biometric signals then this makes the system vulnerable to the replay attack. In the replay attack the recorded signal is replayed to the authentication system thus bypassing the sensor. An example of this includes the presentation of an old copy of a fingerprint image or a previously recorded voice of an authorized user.

Verification fraud attempts to circumvent the system during the process of verification. For example, an attacker may be able to force an authorized user to verify his or her identity to gain access. If an attacker is able to get the pilot to verify his or her identity through force, no one would be able to tell the difference (besides the person who is being attacked and their co-pilot). Enrollment fraud is another possible vulnerability in biometric systems. When a person enrolls his or her biometric data into the system, it must be proven that they really are who they say they are. For example, an attacker may be able to enroll into a system with his or her biometric data but will be known by the system as an authorized user. It will be assumed that some form of identity verification will be performed by authorized personnel prior to user enrollment into the system. The person who is in charge of enrolling biometrics into the database must be trusted and must follow enrollment procedures such as obtaining physical identification of the user who is enrolling their biometric to the system.

Since a biometric system is possibly vulnerable to such attacks it is also possible that the biometric data being transmitted can be vulnerable to another set of similar attacks. Biometric data, stored in a remote location, can be vulnerable to a "man-in-the-middle" attack. If an attacker were to successfully "tap" into the biometric system either in the flight deck, at the remote storage location, or anywhere in-between, then the biometric data being sent across the wires to its destination (for comparison) is vulnerable to capture and replay attacks. Effective countermeasures to this type of attack can include communication protocols requiring encryption and/or digital signatures. Cryptographic techniques to avoid replay attacks may include the use of a nonce value or timestamp associated with the biometric data being sent across the wires. A nonce can be thought of as an opaque token. A nonce/timestamp can be valid only for a certain instance or run of the protocol thus providing resistance to a replay attack on the biometric data. It must be noted that encryption techniques cannot check for liveliness of a signal, so the user must do this at the point of enrollment and at every authentication attempt.

Spoofing can be thought of as defeating a biometric system by introducing fake biometric samples or possibly forcing an authorized user to present his or her biometric to the system. An example of spoofing is using a gummy (fake) finger to fool a fingerprint scanner. Gummy or fake finger attacks may be performed on a biometric system in order to gain unauthorized access to restricted areas by mounting the fake finger against an already stored template of the authorized user's biometric information. Fake finger attacks may also be done during enrollment into the biometric system if authorized personnel are not present during user enrollment. Gummy finger techniques were introduced in part F, section 3 of this chapter. Effective countermeasures to this type of attack are to ensure that the biometric system is capable of performing liveness tests during enrollment and live presentation.

Stored templates are also vulnerable to attack. Stored templates may be tampered or manipulated with at the source of storage (i.e. the database). The database of enrolled authorized individuals can either be local or remote and the database may also be distributed over several servers. In the case of a biometric system employed in the flight deck, the database of enrolled authorized individuals could be in a remote location. On the other hand, an unauthorized individual may try to modify one or more of the biometric representations in the database. This may result in fraudulent individuals being able to gain access to the systems and as well as providing a denial of service to authorized users. One countermeasure to this type of attack is to ensure that the matching and storage device reside at a secure location.

If security policies and procedures are set forth and are well understood then it is possible to become convinced that this system is less vulnerable to many common attacks. This idea is analogous to a computer user who constantly keeps his/her virus signatures updated on his/her system, since they have taken the time to keep their system well monitored and updated then their system is less vulnerable to known attacks.

There are some basic security principles that deserve some attention in relation to a biometric system:

- Users of the biometric system should have the least amount of privileges necessary to complete the job. For example, the subject who is offering his/her biometric to the system for acceptance would have very low to no privileges in terms of the biometric system. However, the user on the other side of the biometric system, who is waiting for the data to arrive for comparison, may have a few more privileges.
- The biometric system must be as small and simple as possible (economy of mechanism). If the system is small and simple, then it would be easier to implement, test, and analyze. Vulnerability testing would be easier to perform because in a complex system, it is more difficult to find deeply hidden vulnerabilities such as unauthorized access paths (however it should be noted that a backdoor put in by a malicious designer in the design phase of the device and/or software to use the device can be virtually impossible to locate [2]).
- Data that is kept in the system (i.e. templates) can be thought of as objects and the users of the system can be thought of as the subjects. With this in mind, any access to objects by subjects should be mediated, logged and/or monitored. Every access to every object by subjects should be checked for privilege (i.e. does this person have the correct credentials to add/delete biometric templates?).

- Physical access to any part of the biometric system should be limited. The database that stores the biometric templates may be located in a physically protected location.

These basic security principles for biometric systems serve merely as a guideline for consideration in regards to requirements for a flight deck biometric authentication system. Ideally we want to be able to prevent any type of attack before it actually happens.

Combining these ideas we can say that the biometric system, together with relevant peripherals at the user interface, should be designed and implemented in such a way so as to render it resistant to physical attack. Ideally, the biometric system or device should be resistant to tampering, and should sense and audit any tampering activity and report it to some central system in order to take appropriate action.

I. BIOMETRIC PERFORMANCE MEASUREMENTS

The performance of biometric systems is tested usually in terms of false rejection rate (FRR), false acceptance rate (FAR), failure to enroll rate (FER), enrollment time, and verification time. The false acceptance rate is most important when security is a priority whereas low false rejection rates are favored when convenience is the priority.

The biometric system employed in the flight deck must have a low false acceptance rate since security is the priority. If the false acceptance rate is as low as possible then we have a better chance of not allowing unauthorized subjects into the system. The point at which the FAR and FRR meet or crossover is known as the equal error rate. This rate gives a more realistic measure of the performance of the biometric system rather than using either the FAR or FRR individually.

The failure to enroll rate (FER) is the rate which a subject is unable to introduce his or her biometric to the system which is acceptable to the system. For example, if there is a fingerprint scanning device which is very sensitive to the images presented to it and a subject is not able to provide a clear cut image then he or she will not be able to enroll into the system. Usually, there are systems that will allow the subject several attempts to enroll biometric information into the system.

Both the enrollment and live presentation times are important factors in determining or testing system performance. The enrollment time is that timeline in between and including the capturing of the biometric sample and creating the stored template of that sample.

The verification time is a measurement of the process of live presentation. This process includes the capture of the raw data, live template processing, comparison of the stored template to the live template and the time it takes for the system to provide a decision (i.e. match or non-match). To provide the continuous authentication mechanism desired for the flight deck, the verification time must be near real time for a successful flight deck biometric authentication system.

III. NEW TRENDS IN BIOMETRICS

A. MULTI-BIOMETRICS

Biometric systems have to contend with noisy data, restricted degrees of freedom, and failure to enroll problems, spoof attacks, and unacceptable error rates. In some situations, it may be feasible to deploy a biometric system that takes advantage of more than one method of identification or authentication to overcome these problems. A biometric device can either be integrated with non-biometric forms of authentication or with other forms of biometric authentication devices. When a biometric device is integrated with other forms of biometric authentication devices, it can be described as a "multi-biometric system". Multi-biometric systems may be more reliable and provide higher verification rates due to the presence of multiple, independent pieces of evidence [6]. Multi-biometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage, and provide anti-spoofing measures by making it difficult for an intruder to steal multiple biometric traits of a genuine user [6].

If there is a weakness in one method of biometrics, then combining it with a biometric method that is stronger with respect to that weakness will alleviate that problem. For instance, it may be feasible to deploy a biometric system in the flight deck that consists of both fingerprint scanning and voice recognition devices. In addition, a multi-biometric system may reduce the false reject rate and the failure to enroll problem [6].

One must determine the logic used by a multi-biometrics system. Each individual biometric method must be incorporated to logically work with the other biometric method that it is being combined with. The logic of the multi-biometric system may be implemented in an AND configuration or in an OR configuration.

If these two devices must work together to provide continuous authentication using the AND configuration, then they both must output a matching score. It is noted in [6] that this type of configuration will reduce the false acceptances achieved by using either device by itself, but it will increase the number of false rejections.

It is possible that these systems may be combined in an OR configuration. In the OR configuration, either device will be able to provide the continuous authentication needed in the flight deck. If the OR configuration is used as noted in [6] then this type of configuration will reduce the number of false rejections, but increase the number of false acceptances. The number of false rejections and false acceptances are based on the matching threshold that the administrators set the device at initially. The matching threshold is used to decide between a genuine user and an impostor.

Usually vendors of biometric devices have suggestions for setting threshold values according to the security level you are trying to achieve. The security level may be labeled as low, medium, and high. Each security level has a threshold value associated with it as well. System performance can be improved by providing separate threshold values for each user of the system. In [19], it is shown that by providing separate threshold values for each user of the system, which consists of a combination of fingerprint, face, and hand geometry, the genuine accept rate is above 96%.

Using multiple biometrics in a system may not be the best solution in some cases. In [15], an example is given where fingerprints and voice were used together as one system. The conclusion from this study is that a strong biometric is better alone than in combination with a weaker one. More analysis and testing of multi-biometric systems is needed in order to be able to draw clear conclusions regarding the implementation of such a system.

A multi-biometric system may increase the certainty that the person is who he claims to be and increases the flexibility and circumstances under which someone can be verified. The accuracy and performance of an authentication system may be increased by employing a multi-biometric system if the most compatible methods are combined together to produce a stronger biometric system (i.e. where weaknesses in one method are complemented by the strengths in the other method). If the results of combining different biometric methods are not fully researched, then it is possible that a layered biometric system may be weaker than using only one method.

1. Multi-Biometric System "AND" Configuration

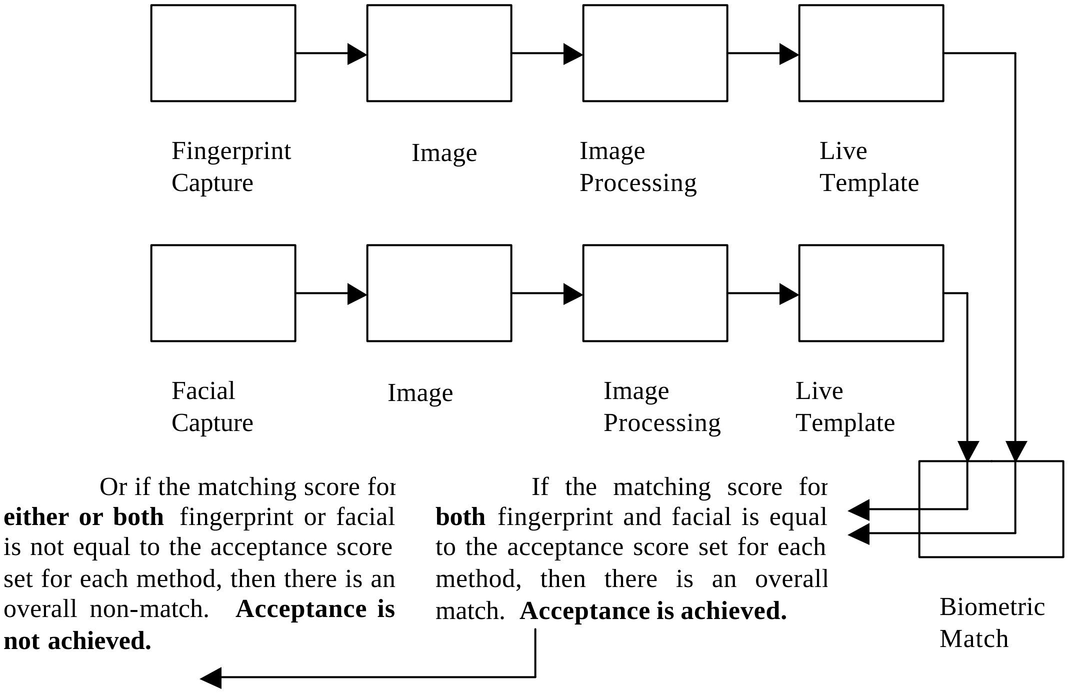

Fingerprint Capture
Image
Image Processing
Live Template
Facial Capture
Image
Image Processing
Live Template
Or if the matching score for **either or both** fingerprint or facial is not equal to the acceptance score set for each method, then there is an overall non-match. **Acceptance is not achieved.**
If the matching score for **both** fingerprint and facial is equal to the acceptance score set for each method, then there is an overall match. **Acceptance is achieved.**
Biometric Match

Figure 1 Multi-Biometric System using the AND configuration

Figure 1 depicts a multi-biometric system using the AND configuration In this configuration, it is necessary that both of the biometric methods achieve a matching score equal to the acceptance score set for the system (which is set up initially). This system would provide high confidence that the person who is introducing their biometric information to the system is who he says he is. Spoofing is more difficult because two biometric characteristics are used. It is possible to set individual biometric thresholds for each method used or to weight one biometric method more than the other throughout the system as a whole.

In [6], some formulas are presented for the false accept and false reject rates in terms of probabilities while using the AND configuration. These error probabilities are denoted as [6]: $P_A(FA)$, and $P_A(FR)$, where $P_A(FA)$ denotes the probability of a false accept while using the AND configuration (P_A) and where $P_A(FR)$ denotes the probability of a false reject while using the AND configuration (P_A).

As explained in [6], if the AND configuration is used to combine the two tests **1** and **2**, a False Accept can only occur if both tests **1** and **2** produce a False Accept. Thus the combined probability of a False Accept, $P_A(FA)$, is the product of its two probabilities for the individual tests:

$$P_A(FA) = P_1(FA)P_2(FA)$$

This formula indicates that the combined probability of producing a false accept would be lower than either of the methods alone. However, as explained in [6], the probability of producing a false reject becomes higher when combining two biometric methods rather than using only one biometric method alone. The formula, as given and defined in [6] is:

$$P_A(FR) = 1-[1-P_1(FR)][1-P_2 (FR)]$$

$$= P_1(FR) + P_2(FR) - P_1(FR)P_2(FR)$$

This formula shows that the probability of producing a false reject would decrease if one used a single biometric method alone, rather than combining multiple biometric methods, especially if one is considerably stronger than the other. Formulas for the OR configuration are similar except that a false reject can only occur if both biometric methods produce a false reject.

2. Multi-Biometric System "OR" Configuration

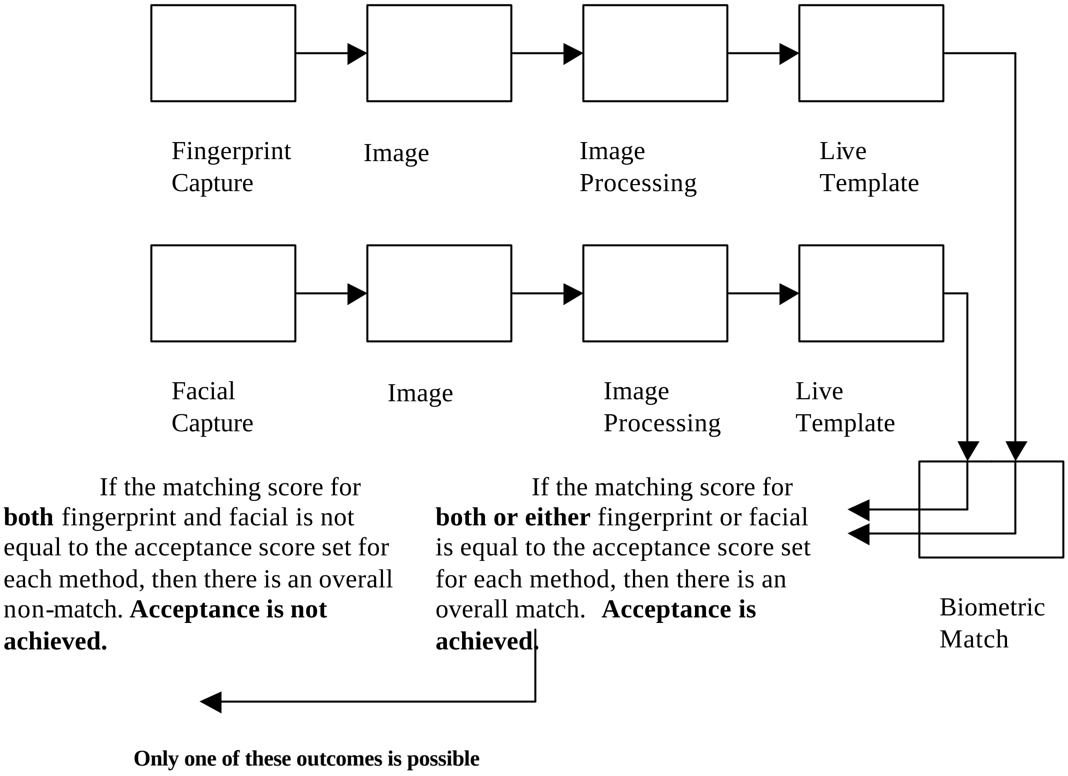

Fingerprint Capture
Image
Image Processing
Live Template
Facial Capture
Image
Image Processing
Live Template
Biometric Match
If the matching score for both fingerprint and facial is not equal to the acceptance score set for each method, then there is an overall non-match. Acceptance is not achieved.
If the matching score for both or either fingerprint or facial is equal to the acceptance score set for each method, then there is an overall match. Acceptance is achieved.
Only one of these outcomes is possible

Figure 2 Multi-Biometric system using the OR configuration

Figure 2 depicts a multi-biometric system using the OR configuration, in this configuration, overall acceptance by the system can be achieved either by both biometric methods possessing a matching score equal to the acceptance score set for the system initially or by either biometric method possessing a matching score equal to the acceptance score set for the system initially. This configuration does not provide the confidence that the person is who they say they are as well as the AND configuration does. This configuration may decrease the false rejection rate overall because the user will be accepted into the system by for example, either their fingerprint template matching the previously stored fingerprint image or by their facial template matching the previously stored facial image or both. Since using this configuration may decrease the false rejection rate, the false acceptance rate will increase, which is not a good idea for highly secured areas.

B. CURRENT BIOMETRIC STANDARDS

In the past, many biometric vendors created proprietary algorithms and unique application programming interfaces, which had similar purposes but different functions and parameters. Because of this, the adoption of biometrics was very slow and they realized that they all needed to adopt a single application-programming interface (API) [30]. The current biometric standards are [30]:

- ANSI/NIST-CSL 1-1993
- FBI WSQ 1993 Image Compression
- CJIS-RS-0010 FBI Appendix F & G
- ANSI/NIST ITL 1a – 1997
- ANSI/NIST ITL 1-2000 SP 500-245
- BioAPI-2001 Specification Version 1.1
- NISTIR 6529-2001 Common Biometric Exchange File Format
- ANS X9.84-2001 Biometric Information Management and Security
- ANSI/INCITS 358-2002 BioAPI Specification Version 1.1

The ANSI/NIST-CSL 1-1993 and ANSI/NIST ITL 1a-1997 are older documents that focused on the use of fingerprints that were a part of the automated fingerprint identification systems for law enforcement. The ANSI/NIST-CSL 1-1993 standard specified a logical record structure for processing mug shot, facial and scar/mark/tattoo image data. The ANSI/NIST ITL 1a-1997 standard is a revision of ANSI/NIST-CSL 1-1993 which specifies a common format to exchange the image data information between dissimilar systems or systems made by different manufacturers. ANSI/NIST ITL 1-2000 SP 500-245 is a revision, re-designation, and consolidation of ANSI/NIST-CSL 1-1993 and ANSI/NIST-ITL 1a-1997.

ANS X9.84-2001 defines the requirements for managing and securing biometric information for use in the financial industry. X9.84 specifies cryptographic message formats and key management techniques that can be used to provide data integrity, authentication, and privacy for biometric matching. The X9.84 standard defines a set of mandatory requirements to manage biometric information securely. This standard is focused on the security of biometrics. This standard is not scheduled for revision until 2004.

Familiar high level abstractions such as enroll, verify, and identify and primitive functions such as capture, process, match, and create template are defined by an application programming interface (API) in the BioAPI Specification, version 1.1, 2001. This specification also defines a common data structure, which is called the Biometric Information Record that is used by an application as the input and output to the Biometric Service Provider. The wavelet/scalar quantization (WSQ 93) algorithm1 is the FBI standard for digital fingerprint compression. CJIS-RS-0010 FBI Appendix F & G is a specification for fingerprint transmission.

As newer biometric methods emerge and current methods are enhanced, more standards will emerge as well. Many of the current biometric vendors look at the X9.84 standard for security. Few of the biometric vendors have begun to implement security methods into their applications to protect biometric information. Several biometric vendors have had assessments of their products, with the goal of passing an X9.84 examination sometime in the near future [30].

C. BIOMETRIC SYSTEM STUDIES

1. The National Physical Laboratory Communications Electronic Security Group (CESG) [23]

The National Physical Laboratory Communications Electronic Security Group (CESG) evaluated seven biometric systems from the period May to December 2000. The CESG performed these system tests in a normal office environment. They tested face, fingerprint, hand geometry, iris, vein, and voice recognition systems. Two fingerprint systems were tested, one of which was based on a fingerprint chip (i.e. smart card) and the other was based on an optical system. The results from the vein-based systems will not be examined.

The systems that were tested by CESG are:

- Visionics – FaceIt verification demo (face)
- Fingerprint recognition system (optical)
- HandKey II (hand geometry)
- Iridian Technologies – IriScan System 2200 (iris)
- OTG – Secur PBX demonstration system (voice)

CESG used over 200 participants in this study ranging in ages 18 – 65 + which included both males and females. There was a little bit more distribution of males in all of the age categories. The failure to enroll rates that are recorded by CESG are given in Table 3:

System	Failure to Enroll Rate
Face	0.0%
Fingerprint	2.0%
Hand	0.0%
Iris	0.5%
Voice	0.0%

Table 3. Failure to enroll rate

The false acceptance and false rejection rates are reported in a graph with respect to the threshold value. They are calculated as follows:

- FAR (t) = (1 – FTA) FMR (t)
- FRR (t) = (1 – FTA) FNMR (t) + FTA

Where FTA is the failure to acquire rate, FNMR is the false non-match rate, and FMR is the false match rate. The false match and non-match rates are used to measure the accuracy of the matching process. *t* represents the decision threshold. The *decision threshold* is the value, set initially, to determine whether a user is accepted or rejected by the system, according to their matching score. The *failure to acquire rate* measures the proportion of attempts for which the system is unable to capture or locate a sufficient quality image. This may happen simply when the image that was captured doesn't meet the quality requirements of the system.

The failure to acquire rates as recorded by CESG are given in Table 4:

System	Failure to acquire rate
Face	0.0%
Fingerprint	0.8%
Hand	0.0%
Iris	0.0%
Voice	2.5%

Table 4. Failure to acquire rate

These tables exclude instances of user errors such as not correctly positioning fingers on the fingerprint device. According to the graphs provided in the final report, the false accept rates as recorded by CESG are given in Table 5:

System	False acceptance rate
Face	0.23%
Fingerprint	0.18%
Hand	0.4%
Iris	0.0%
Voice	0.01%

Table 5. False acceptance rate

In this study, there were no indications as to what the false rejection rates were for these and corresponding methods. The method with the highest failure to enroll rate was the fingerprint recognition system. The reason for this high rate is usually due to the particular biometric technology being unable to read the characteristics of a given person for various reasons. Influences which may affect the outcome of a fingerprint recognition system, including the enroll rates, are mentioned in Chapter II, section 2 of part F. Most of the methods that were tested had failure to enroll rates at 0.0%. Having a low failure to enroll rate is an ideal attribute in a biometric system, all of the users should be able to register their biometric to the system in order to be able to use it effectively.

The method with the highest failure to acquire rate was voice authentication. There are various reasons why this rate was so high. One reason may be because the voice that was introduced to the system did not meet the quality requirements of that particular system. Next in line to voice was fingerprint with a failure to acquire rate of 0.8%. The rest of the methods tested had a 0.0% failure to acquire rate. Failure to acquire rates may lead to higher false rejection rates for authorized users. The failure to acquire rate is difficult to predict or prevent because it is a factor that is not controlled by the system or the users (we cannot tell when enrollees will not be able to provide an acceptable biometric sample to the system).

The only method that had a 0.0% false acceptance rate was iris scanning. The rest of the methods and vendors that were tested were all under 1% for false acceptance rates. Ideally, a system should have a low false acceptance rate because then that would mean that it would be less likely that the system would allow an impostor to gain access to the system or to take control of the flight without being noticed. The only rates that were not reported in this study were for the false rejection rates. The false rejection rates may be calculated from the given information.

It is important that one does not overlook these types of error rates in a biometric authentication system. One way to compare systems is through the testing of these rates. Since we are able to make comparisons with several products and vendors, we will be able to make the choices that best fit our needs. There are many products and competition is increasing, which means that costs may be decreasing. More exhaustive tests are needed for all of these products so that we are able to choose the most beneficial system for our purposes.

2. Multi-Biometric System Tests

L. Hong and A.K. Jain [15] developed a prototype that integrates faces and fingerprints in authenticating personal identification. Their proposed system overcomes the limitations of both facial-recognition and fingerprint-verification systems. In order to test their proposed system, they used the MSU (Michigan State University) fingerprint database and a public domain face database. There are a total of 1,500 fingerprint images of size 640x480 in the MSU fingerprint database. The 1,500 fingerprint images come from 150 individuals who have 10 images each. These fingerprint images were captures with an optical scanner manufactured by Digital Biometrics.

The face database has a total of 1,132 images of 86 individuals. Of the total images, 400 came from the Olivetti Research Lab, 300 came from the University of Bern, and 432 came from MIT Media Lab. The images are re-sampled and given a fixed size of 92x112. A total of 590,000 (590 x 1000) face and fingerprint test pairs were generated and tested. The details of this particular test are explained in [15]. The table below describes the false reject rates (FRR) for various values of false accept rates (FAR) for face, fingerprint, and integrated face/fingerprint. As table 6 indicates, the false rejection rate is lower for every false accept rate value for an integrated system. This system is integrated with face and fingerprint technology.

Table 6. False Reject Rate vs. False Accept Rate in an integrated system

False Accept Rate	**False Reject Rate (FRR)**		
	Face	**Fingerprint**	**Integration**
1 %	15.8 %	3.9 %	1.8 %
0.1 %	42.2 %	6.9 %	4.4 %
0.01 %	61.2 %	10.6 %	6.6 %
0.001%	64.1 %	14.9 %	9.8 %

Having reviewed a variety of biometric techniques, the next chapter will present two designs for in-flight biometric authentication systems.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PROPOSED DESIGN FOR IN-FLIGHT BIOMETRIC SYSTEM

The intent of the flight deck biometric authentication system is to provide a strong guarantee of identification. The system must provide assurance that the identity of the person is correct and that the identity is unique. Requirements for the flight deck biometric authentication system include reliability, ease of use, and non-intrusiveness. The authentication system should provide continuous and accurate operation. Authorized users should be allowed access and unauthorized users should be prohibited, without interruption or deterioration in performance, accuracy or speed.

The biometric device or system of devices onboard the aircraft must be physically secured such that it does not become vulnerable to attack, theft, or tampering. Controlled access to the flight deck can be achieved by implementing a biometric device outside of the flight deck doors as suggested in this study. A clear and concise set of security policies for the use of the biometric system must be defined and set in place. The main reason for these security policies is to ensure that the operation and security of the biometric system is adequate.

Periodic inspection of the system will be necessary to ensure proper functioning under any type of conditions. Lastly, even if layered biometrics is employed in the flight deck, the system, as a whole, is required to be small and easy to understand. This non-complex design of the biometric authentication system will be useful in the event of a system failure. In such an event, if the system is small and easy to understand it will be easier to restore even under extreme conditions.

A. BIOMETRIC SYSTEM PROCESS

All biometric systems basically follow the same set of processes for biometric feature matching represented in Figure 3.

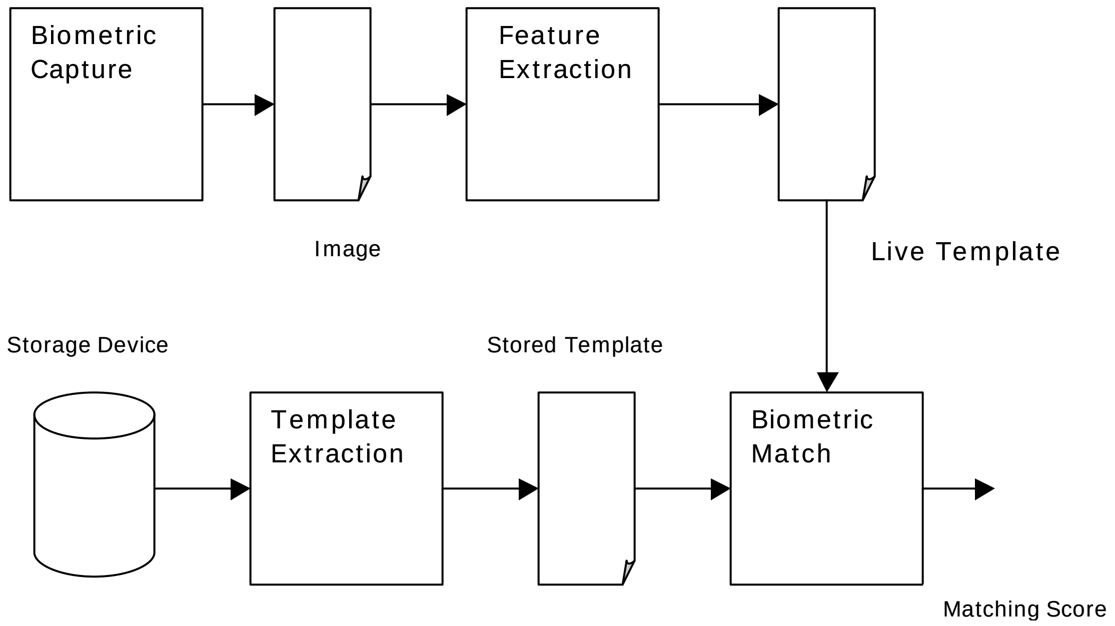


Figure 3 Basic Biometric System Process

Biometric capture takes place at the biometric device (i.e. fingerprint scanner). The image of the biometric is processed using specific algorithms tailored for that biometric method to produce a live template. The live template of the biometric is a numerical representation of the currently acquired biometric. From the storage device, the template of the biometric which was stored as part of user enrollment, is retrieved and should match the value from the live template. When this occurs a biometric match is acquired.

B. PROPOSED DESIGNS FOR BIOMETRICS IN THE FLIGHT DECK

1. Design #1

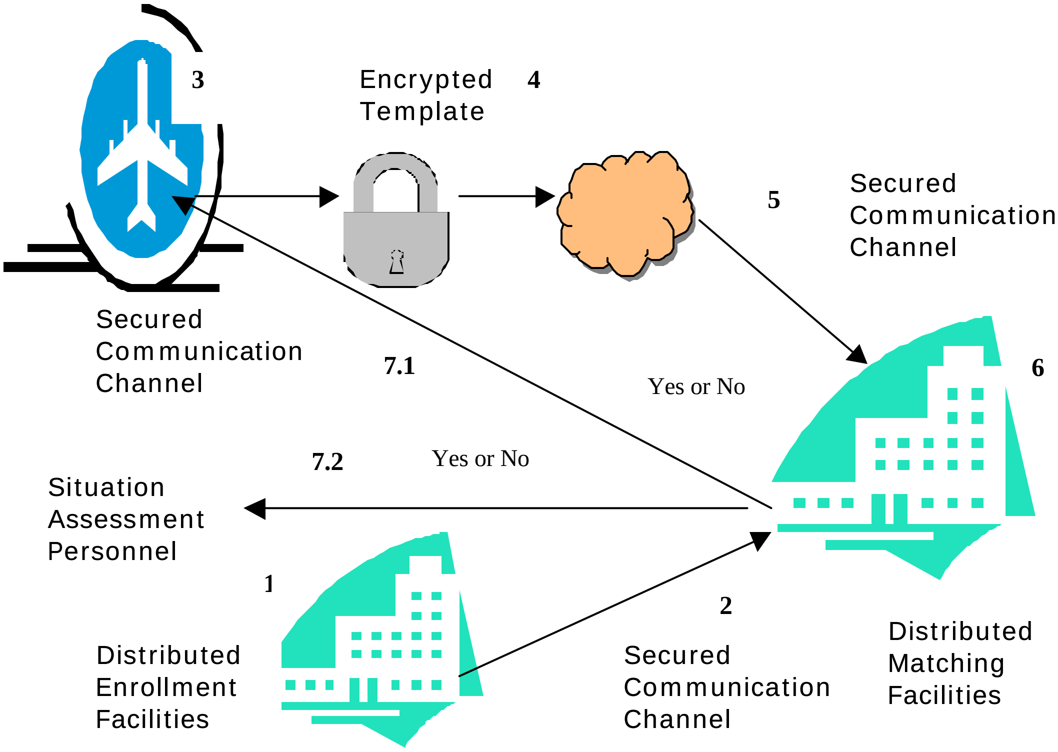

3
Encrypted Template
4
5
Secured Communication Channel
Secured Communication Channel
7.1
Yes or No
6
7.2
Yes or No
Situation Assessment Personnel
1
2
Distributed Enrollment Facilities
Secured Communication Channel
Distributed Matching Facilities

Figure 4 Proposed Design #1

As shown in Figure 4, the process of a biometric system is a little more complicated than that of just the basic biometric system process. These processes are labeled to show the order in which certain activities take place. Label 1 in Figure 4 represents the distributed enrollment facilities. The distributed enrollment facility is where the subject will enroll his/her biometric characteristic to the system for the first time. The enrollment process is fairly simple because this is where the ID of the person is checked physically (i.e. drivers license) and their biometric information is entered into the database of authorized biometrics. The enrollment facilities are distributed such that the subjects are not confined to the use of one centralized enrollment location. Each enrollment facility will have the same authorized user database as the other enrollment facilities in order to provide redundancy. Redundancy avoids a single point of failure.

Label 6 in Figure 4 represents the distributed matching facilities. This is where the stored biometric templates, transferred from the enrollment facilities (label 2) are compared against the live biometric templates that are transferred from the flight deck (labels 3, 4, and 5). Labels 3, 4, and 5, in Figure 4 represent the live biometric template that is encryp ted and communicated to the distributed matching facilities via secured communication channels. At the matching facility, the stored and encrypted biometric template is decrypted and compared to the live template that was received from the flight deck of the aircraft (label 6). It is necessary to have distributed matching facilities such that all of the different flight decks that are sending information are not confined to sending biometric templates to one facility, thus possibly causing a communication channel or processing bottleneck.

The physical location of the biometric device(s) is within the flight deck (Figure 4, label 3). This is where the authorized user attempts to authenticate. This authentication process is as follows:

- Authorized user introduces his/her biometric information to the biometric device
- The biometric device captures the biometric information
- An image of the biometric information is extracted, which is represented numerically
- The image goes through processing using an algorithm tailored to the specific method of biometrics used.
- A live template is then extracted, which is also represented numerically

Once the live template is captured, it must be encrypted and is sent through the communications channel to the matching facility securely. Once a match is made, the appropriate matching facility will send an acknowledgement message back to the authorized user in the flight deck. This acknowledgement, which is sent from the matching facility back up to the flight deck (Figure 4, label 7.1), may not be necessary; this depends upon the overall design. Sometimes matches between the live and stored biometric templates are not possible. In this case, there are two possible feedback messages. The first one may be a "retry" message, prompting the authorized user to re-enter his/her biometric information. This feedback message may be logged by the system. The second feedback message is related to an authentication failure. This authentication failure message will be logged and sent to appropriate situation assessment personnel, which can include stewardess, air marshal, or ground personnel.

It is important to note that the matching results, positive or negative, may be reported to situation assessment personnel on the ground (or elsewhere) and not to the personnel in the flight deck; or the matching results may be reported to both the situation assessment personnel (Figure 4, label 7.2) and the flight deck crew (Figure 4, label 7.1), depending on policies and design. There are many similar situations that may take place, but it is not feasible to go through every possible situation in this study.

The authentication, matching, and acceptance (or rejection) can all take place inside of the flight deck. This scenario would eliminate the need for the secure communication channel between the matching facilities and the flight deck; thus eliminating any vulnerability associated with the communication channel.

A second proposed design follows from Figure 4 with some small modifications. In the second design both the distributed matching and enrollment facilities would still exist, but an additional matching device would be needed in the flight deck in order to accomplish live presentation, matching, and acceptance (or rejection) onboard the aircraft. The device that would be required to have in the flight deck is a trusted, hardened, and tamperproof PC. Below are reasons why we would need a PC onboard the aircraft:

- The distributed enrollment facilities will maintain DVDs that contain all biometric templates used for authentication in the flight deck. The DVDs will include a copy of the database of existing and new biometric templates that have been introduced to the enrollment facilities.
- These DVDs would be distributed between the distributed matching facilities and the various aircrafts that have the trusted and tamperproof PCs onboard.

- The trusted and tamperproof matching device will be onboard the aircraft along with the biometric device. Thus it is possible to authenticate, match, and reach acceptance in the flight deck in near real time.
- Once acceptance is reached in the flight deck, someone on the ground or in the aircraft (e.g. air marshals or stewardess) will be sent a signal (yes or no) letting them know if authentication and matching were successful onboard the aircraft. This process is shown in more detail in Figure 5.

2. Design #2

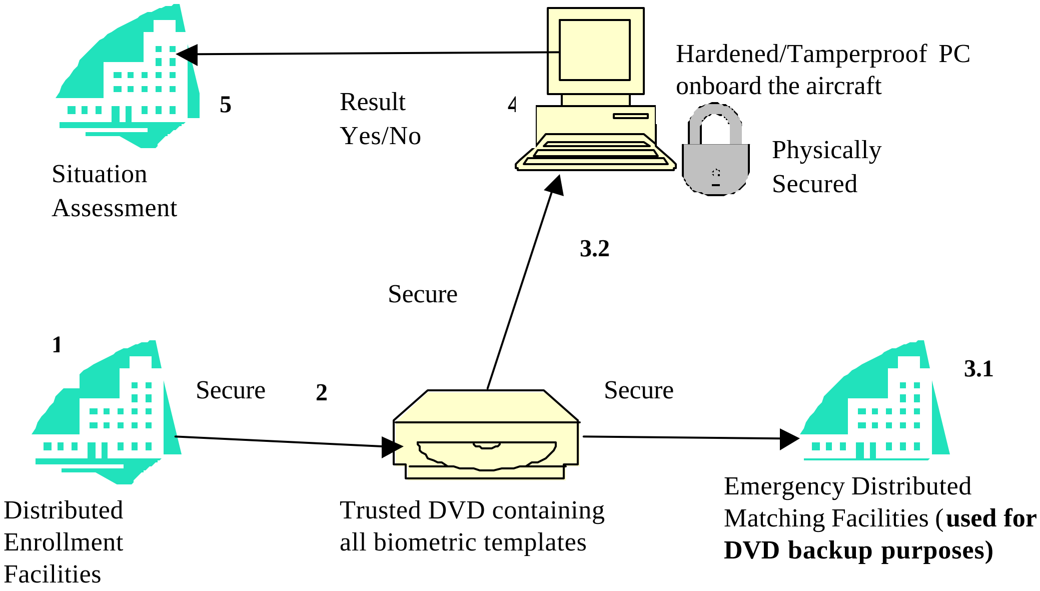


Figure 5 Proposed Design #2

Figure 5 depicts the second design scenario for employing flight deck biometric authentication. In this scheme, as compared to Design #1, there is no need for the two secured communication channels between the matching facilities (Figure 5, label 3.1) and the aircraft (not shown here). Just like Design #1, Design #2 also contains the distributed enrollment and matching facilities (Figure 5, labels 1 and 3.1). The distributed enrollment facilities serve the same purpose as in proposed Design #1. However, the emergency distributed matching facilities in Design #2 are where the DVDs are kept and will be used as a backup in the event of an emergency (e.g. if something happens to the PC onboard the aircraft then the authorized personnel will still be able to perform matching by communicating with the matching facility). The same security policies that were described for Design #1 also apply here.

The biometric device is responsible for acquiring the user's biometric data and in both designs this device is in the flight deck. In Design #2, as opposed to Design #1, a matching device is onboard the aircraft (but not necessarily inside the flight deck). Either the matching device or the actual biometric device can be the feature extraction unit.

The matching device includes trusted DVD media that contains updated biometric template databases, generated at the enrollment facilities. Both the aircraft and the distributed matching facilities have these DVDs and the enrollment facilities distribute updates when necessary to the appropriate locations. It is not exactly known how often the biometric database will change, but it is important that each aircraft has the most recent copy of the database onboard the aircraft and the DVDs that contain old information are destroyed.

The secure handling of the DVDs must be taken into consideration since they contain valuable information. These DVDs will only be produced at the enrollment facilities and will be physically protected until they are distributed to the emergency matching facilities and the matching device onboard the aircraft, as shown in Figure 5, label 3.2. The actual process of exchanging this DVD from the source to the flight deck is not discussed in this study, but it is important that this DVD must be exchanged from the source to the flight deck securely so that we are ensured that the DVD has not been tampered with or exchanged with counterfeit DVDs containing false information.

The matching device onboard the aircraft, as shown in label 4 in Figure 5, should contain its own backup system and a backup battery pack in the event of a power failure. Since the PC onboard the aircraft is not connected to any other outside device, it is not vulnerable to common network attacks. The location of the PC within the aircraft may pose a vulnerability. If the PC is readily viewable, then it becomes vulnerable to theft, but as shown in Figure 5, the PC is physically secured. One requirement for the PC onboard the aircraft is that it is tamperproof. One should not be able to tamper with the PC thus making any information contained within it vulnerable to theft or modification. This PC should contain as few applications as possible. For example, one may want to have a basic operating system along with the corresponding software needed to use the biometric device. All unnecessary services such as telnet, ftp, and http should be disabled in order to eliminate any vulnerabilities present in those applications. The physical security and tamperproof properties of the onboard PC are analogous to the physical security and tamperproof properties of the onboard black box. The integrity and security of this PC will remain at a high level since unauthorized personnel or the general public will not be aware of the physical location nor what it is used for.

The user may be able to digitally sign their biometric information at the time of enrollment with a smart card, for example, to add another layer of security to the biometric template. The smart card can then be presented to the system at the time of live capture, as well as for enrollment.

3. Enrollment Facility: Initial Identification and Enrollment

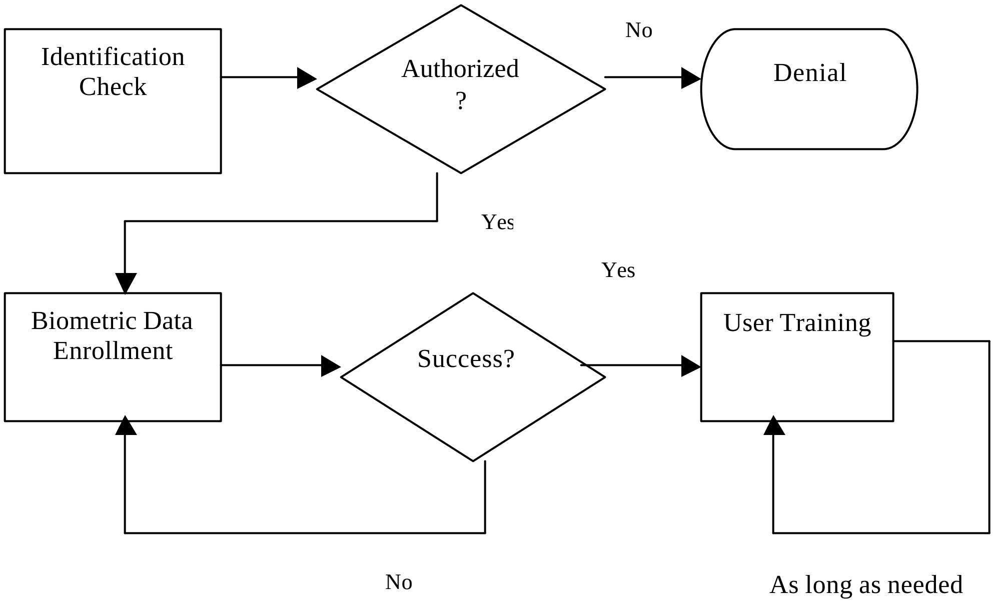


Figure 6 Enrollment facilities initial Identification and Enrollment Process

Figure 6 represents the initial enrollment process that takes place at the distributed enrollment facilities. Initially, the authorized person in charge at the various enrollment facilities is responsible for physical identification checking of the potential biometric system users (i.e. photo ID). Once the authorized personnel positively identify the legitimate user, they are allowed into the system; otherwise they are denied enrollment access and must provide adequate identification. Once the user's biometric information is accepted by the biometric device it will be placed in the database and they will receive training on how to properly use the device in the flight deck. This whole process will be identical at all of the enrollment facilities. The biometric device(s) will be physically secured and audit logs will be performed in order to keep track of the number of users who enroll their biometric data into the database.

The user training process will take as long as the user feels fit. It may take a while for some users to become comfortable with the device(s) and they may need more training time. On the other hand, other users will be very comfortable with the device(s) and will need less training time. The users will be fully trained prior to implementation and use of the flight deck biometric authentication system. It is also possible that a training class could be provided for several users at one time.

4. Enrollment Facility: Biometric Data Enrollment to Trusted DVD Storage

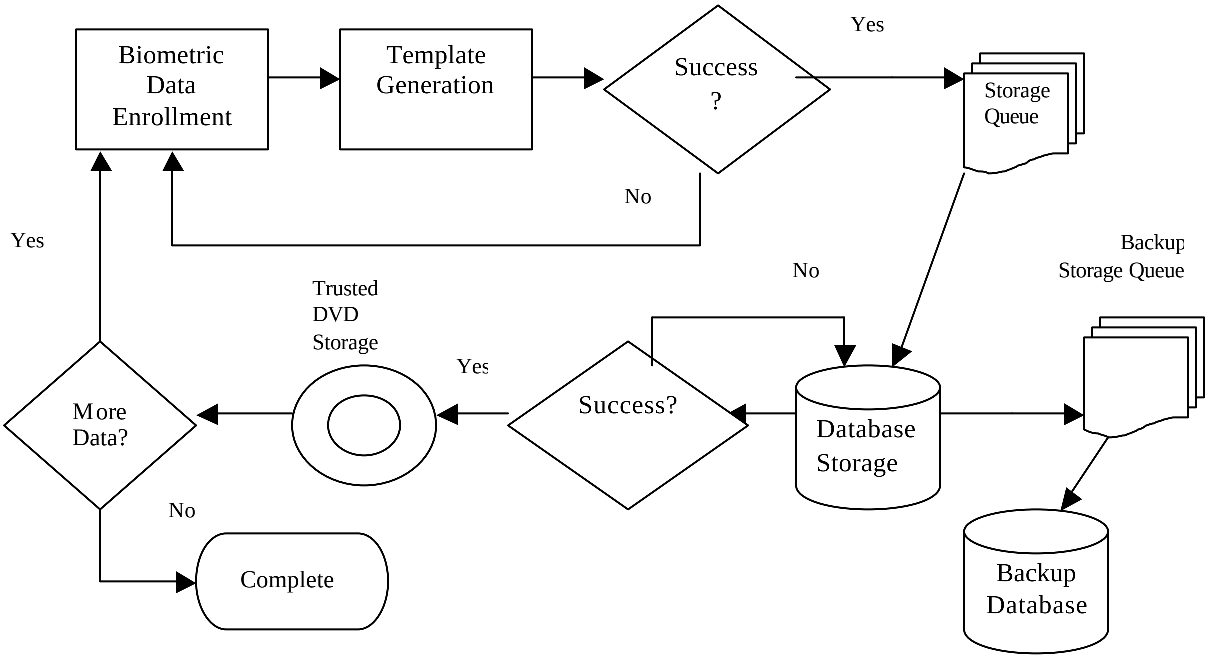


Figure 7 Biometric Data Enrollment to Trusted DVD Storage Process for Design #2

Figure 7 represents the process that occurs between biometric data enrollment and DVD storage of the template. This process begins with the biometric data enrollment. Once the device has captured the biometric data, a template is generated. This template will be used later for comparison at the time of authentication/matching. If the biometric data is not successfully converted into its equivalent template then the biometric data must be re-enrolled into the system. After the biometric data has been converted into its equivalent template, it will be stored into the database, along with the biometric templates of other authorized users. If there is a problem with the database storage, the process of capturing the biometric from the user and storage is attempted again until success has been reached. When the database storage of the template is successful, the biometric template will be stored into the backup database at the enrollment facility and then stored into a trusted DVD. This process corresponds to the proposed Design #2, where a trusted DVD is needed at both the matching facilities and onboard the aircraft.

When multi-biometrics is used, multiple types of biometric data must be stored on the DVD; the user will simply enroll additional biometric data into the system which will go through the same process again.

There are various loops in this process in order to alleviate problems. For example, if there is a biometric template awaiting storage into the database and it is not properly stored, the storage is attempted again until there is success or else the process must be started all over again. Also included in this process is a storage queue. This queue will be useful when several users are enrolling their biometric data and they all reach the storage area at the same time. If a queue were not available, that would restrict this system to storing only one template at a time, which is inefficient.

5. Trusted DVD Distribution

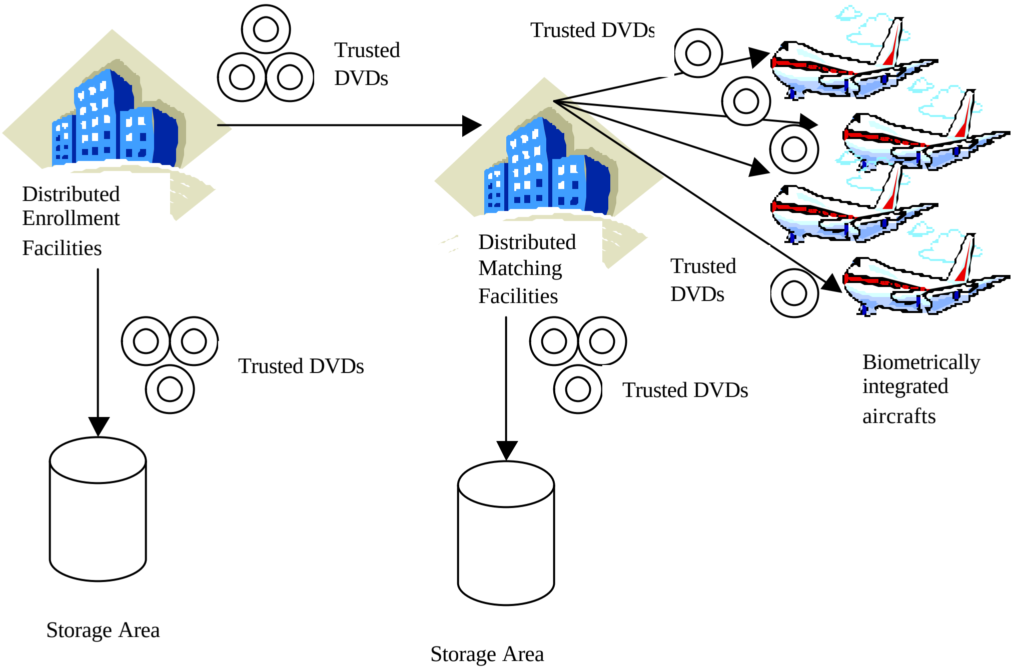

Trusted DVDs
Trusted DVDs
Distributed Enrollment Facilities
Distributed Matching Facilities
Trusted DVDs
Trusted DVDs
Trusted DVDs
Biometrically integrated aircrafts
Storage Area
Storage Area

Figure 8 Trusted DVD Distribution Process for Proposed Design #2

Figure 8 shows the process of DVD distribution from the enrollment facilities to the matching facilities and then to the biometrically integrated aircrafts. Each of the enrollment and matching facilities will keep a storage area for the trusted DVDs for the purpose of redundancy and backup. It is assumed that the DVDs will be conveyed to the different areas securely. Each DVD will be taken to the area where the trusted PC resides onboard.

6. Authentication Onboard the Aircraft (SINGLE BIOMETRIC DEVICE)

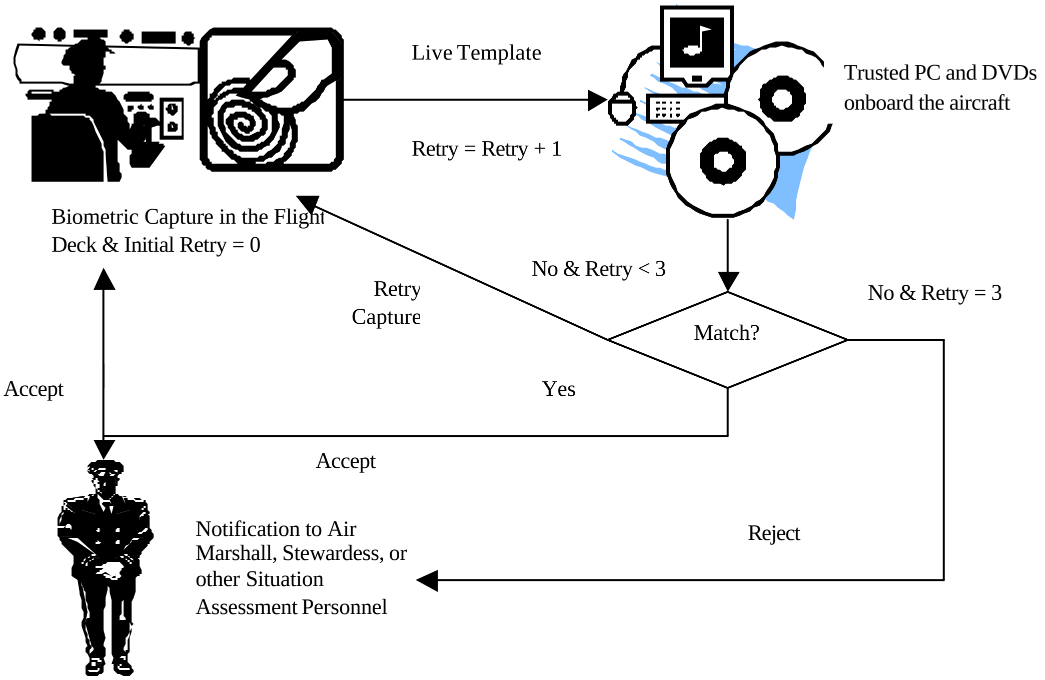

Live Template
Retry = Retry + 1
Trusted PC and DVDs onboard the aircraft
Biometric Capture in the Flight Deck & Initial Retry = 0
No & Retry < 3
Retry Capture
Match?
No & Retry = 3
Accept
Yes
Accept
Notification to Air Marshall, Stewardess, or other Situation Assessment Personnel
Reject

Figure 9 Process of Single Biometric Authentication Onboard the Aircraft for Proposed Design #2

Figure 9 represents the process of authentication using a single biometric device onboard the aircraft assuming the implementation of Design #2. The pilot or co-pilot will perform biometric authentication inside the flight deck via the biometric device. The trusted PC onboard the aircraft will receive the biometric template and will perform matching. Since there may be a mistake in the capture of the biometric, depending on the method, its capture error rate, and the security policy of the organization, the user may be given at least 3 chances for biometric capture in the flight deck. The number of chances for the user to introduce his/her biometric to the device is not limited to 3 (although that is very typical).

In the event of acceptance, a notification will be sent to both the user of the biometric device in the flight deck (or another person in the flight deck) and another authorized person (i.e. Air Marshall or Situation Assessment Personnel who may or may not be at a remote location). This process of authentication in the flight deck can either be used for continuous authentication (i.e. with a video camera for facial recognition) or for periodic authentication (i.e. the pilot or co-pilot introducing their fingerprint to a fingerprint scanner every *n* times within *m* seconds or minutes, where *n* and *m* will be defined according to the biometric method used).

In the event of a rejection, a notification will be sent to both the user of the biometric device inside the flight deck and another authorized person, as described above. The only difference here is the fact that the user will be given *c* chances to authenticate in the flight deck. In figure 9, *c* is 3 times and *c* is incremented every time an attempted biometric data capture is done. If the value of *c* is equal to 3 (in this example) then notification will be sent to situation assessment personnel and proper action will be taken.

7. Authentication Onboard the Aircraft (Multi-Biometrics) "AND" Configuration

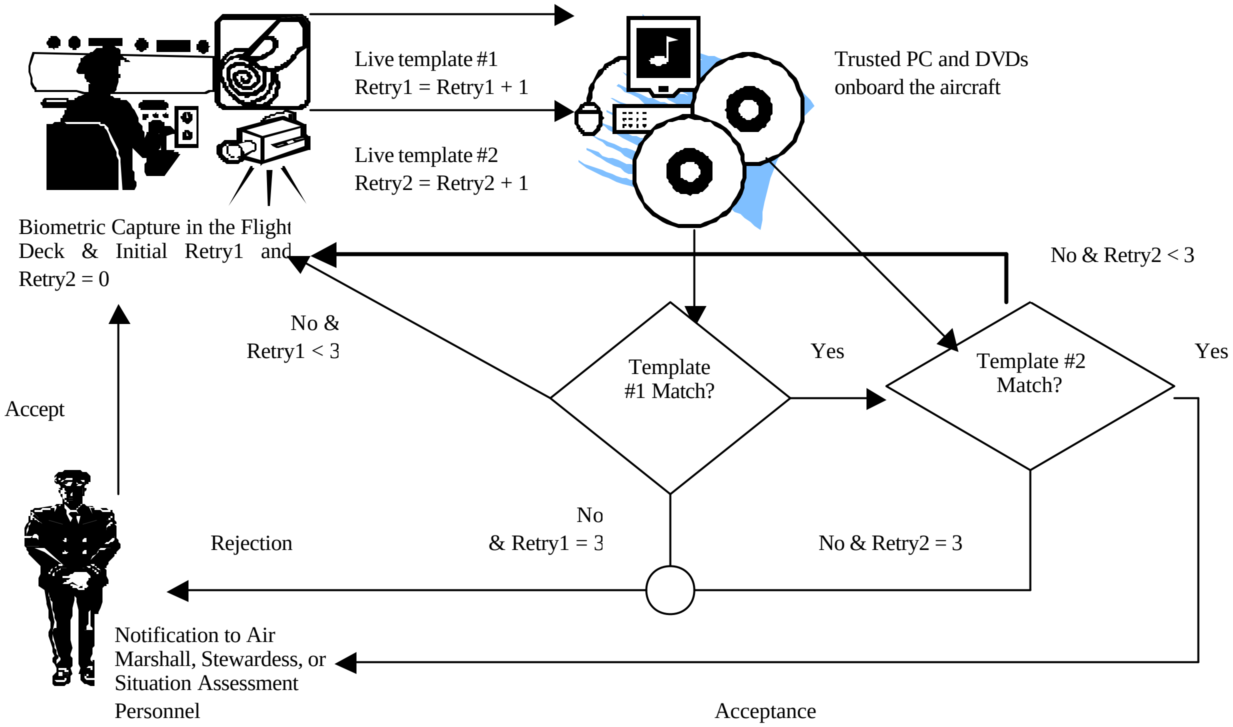


Figure 10 Process of Authentication Onboard the Aircraft using Multi-Biometrics with the AND Configuration for Proposed Design #2

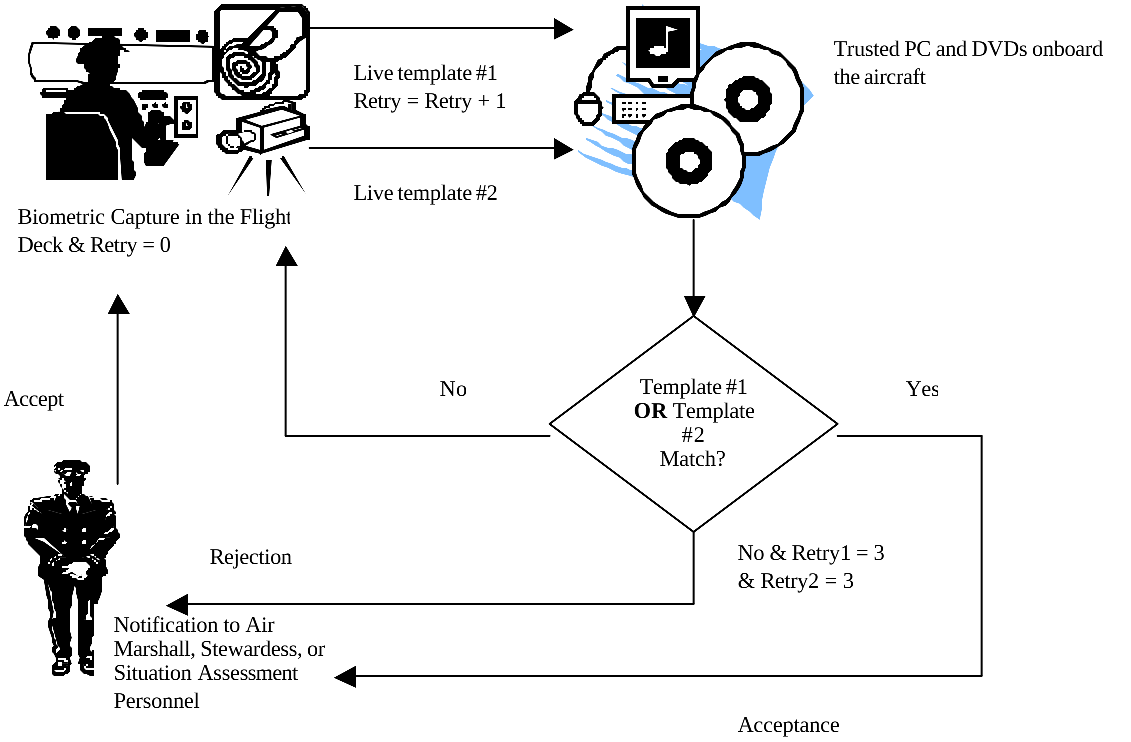
Figure 10 represents the use of multi-biometrics in the flight deck using the AND configuration. This process requires the use of two or more biometric methods in the flight deck. This example shows the use of two biometric methods (e.g. fingerprint scanning and facial recognition) although we are not restricted to only using two methods (the system becomes more complicated), nor are we restricted to only using these two methods (we can have a combination of any biometric methods together). In this example, there are two templates generated, template #1 and template #2. Also, there are two variables declared, retry1 and retry2. These variables are used to keep a count of the number of attempts that the user has tried each biometric method. Every time the templates are sent to the trusted PC, the values of retry1 and retry2 are incremented (their initial values are set to zero). As described in the previous example, the user may be given at least *x* number of chances to authenticate just in case there are problems with the initial or second authentication attempt. The AND configuration requires that there be a positive match from both of the biometric methods with no exceptions.

As this example shows, each template is sent to the trusted PC onboard the aircraft for matching. Ideally, if there is a positive match for both biometric methods on the first try, the user is accepted and notification is sent to another authorized person such as a stewardess, air marshal, or situation assessment personnel who may or may not be in a remote location. It does not matter which biometric data is presented to the system first.

In the event that one biometric method has a positive match and the other one doesn't, the user will be given a number of chances to provide an adequate sample to the system and they will not have to introduce the biometric data which has been positively matched again, only the data which has not been positively matched. If the user cannot authenticate with either one of the biometric methods, they are rejected by the system, notification is sent to the appropriate personnel for action.

The presentation of each form of biometric data to the devices does not have to be done in parallel (i.e., the user should not have to be speaking and presenting their fingerprint at the same time) although acceptance from the system requires two or more positively matched biometric traits. The use of multi-biometrics in the AND configuration may be able to enhance the needed positive identity of who is flying the aircraft since it is more difficult to "steal" two different biometric traits from the authorized user and successfully gain a match from both.

8. Authentication Onboard the Aircraft (Multi-Biometrics) "OR" Configuration



Live template #1
Retry = Retry + 1
Live template #2
Trusted PC and DVDs onboard the aircraft
Biometric Capture in the Flight Deck & Retry = 0
Accept
No
Template #1 **OR** Template #2 Match?
Yes
Rejection
No & Retry1 = 3 & Retry2 = 3
Notification to Air Marshall, Stewardess, or Situation Assessment Personnel
Acceptance

Figure 11 Process of Authentication Onboard the Aircraft using Multi-Biometrics with the OR Configuration for Proposed Design #2

Figure 11 represents the process of authentication in the flight deck using multi-biometrics with the OR configuration. Here, the user in the flight deck does not need to have a match for both of the biometric traits introduced to the device. Only one biometric trait has to be positively matched for overall acceptance. The variables *retry1* and *retry2* are similar to the previous AND configuration and are incremented and used the same way. The user in the flight deck is given a number of chances to introduce his/her biometric to the device for positive matching. If the user has retried both biometric traits at least three times (in this example) then he or she is rejected by the system and notification is sent to appropriate personnel. This process is simpler than the AND configuration in that the user in the flight deck does not need to have two or more positive biometric matches and the restrictions are lessened.

9. Flight Deck Biometric Authentication System Configuration Summary

Sections 7 and 8 describe different scenarios in which the flight deck biometric authentication system can be configured using multi-biometrics. The simplest design comes from implementing one biometric device in the flight deck and implementing a trusted PC onboard the aircraft for matching purposes. If only one biometric device is used in the flight deck, there would be no need for the different configurations as described for multi-biometrics.

The AND and OR configurations are described and their processes are graphically depicted to show how much they differ from each other. Multi-biometrics introduces complexity but also introduces choices. These choices arise from deciding which biometric methods to combine to deciding which configuration to use for the combined methods. These examples represent a general idea on how the process works and do not confine the designer to a particular set of biometric methods. Once there have been more studies in the area of multi-biometrics, it will be easier to combine the most compatible biometrics and there may be more choices available as multi-biometrics continues to mature.

In these scenarios, the process of matching is done onboard the aircraft. This is made possible by integrating a trusted PC somewhere in the aircraft, as described in the discussion of proposed design #2. This PC does not necessarily need to be in the flight deck, it can reside anywhere in the aircraft as long as it is protected from theft or modification. Furthermore, the notification of acceptance or rejection messages do not need to be relayed to the personnel in the flight deck; this depends on how the final design is implemented; however, the notification of acceptance or rejection does need to be relayed to a person external to the flight deck. It is also possible to have a system that will only log acceptances, raising a flag when a rejection occurs. Whether a single biometric method or multi-biometrics is used, there are many possibilities as to how they can be implemented.

The processes for proposed Design #1 would be similar to Design #2, except that there is not a trusted DVD mechanism and there would not be a trusted PC onboard the aircraft. Once the pilot and/or co-pilot introduce their biometric to the device in the flight deck, their biometric template would need to be communicated back to the distributed matching facilities for matching.

10. Comparison of Proposed Designs

Design #2 is simpler than Design #1 because of the absence of the secure communication channels. Both designs contain an extra entity; this extra entity is the situation assessment personnel, who will receive the result of authentication attempts from the flight deck. There are different ways in which the results can be relayed to the appropriate personnel. Relay of this message can be as simple as sending a page to a pager or sending a telephone call to the appropriate situation assessment personnel. As mentioned in Design #1, it may not be necessary to relay every single acceptance to the situation assessment personnel because it simply may not be necessary. On the other hand, it may be practical to relay every rejection from the system in order to take appropriate action. Depending on how the biometric response system is set up, rejection results may need to be conveyed back to the flight deck so that the user has additional chances to authenticate. The biometric system on board the aircraft, whether it is a single biometric system or a multi-biometric system, should allow authorized personnel multiple chances to authenticate because not all attempts will be perfect.

Proposed design #1 appears to be secure, if implemented correctly. The main problem with this design is the need for more secured communication channels, which may allow the biometric process/system as a whole to become more vulnerable to various types of attacks. This design may be used with a single biometric system or with multi-biometrics. If one does not feel comfortable in having a secured PC on board the aircraft, as proposed in Design #2, then this can be thought of as an alternate design scenario.

One type of overhead added to Design #1 is encryption of the biometric templates conveyed to the matching facilities. Encryption is a good mechanism, but it also has its own set of vulnerabilities. There are both weak and strong encryption schemes and if an extremely secure and strong encryption scheme were to be employed, it would be at the cost of processing and communication time. Is it necessary to encrypt the result from the biometric system as it is being conveyed between the matching facilities and the flight deck? If this were necessary, then it would also be at the expense of processing time.

Design #2 seems to be the most feasible solution, because of its simplicity. This simplicity may reduce some of the vulnerabilities that were present in Design #1. First of all, there is no need for encryption of the biometric templates, since they are not being relayed to external destinations. Since the matching process is done in the aircraft, there is no need to worry about man in the middle attacks while relaying biometric template information to the distributed matching facilities. The only process that is not done onboard the aircraft is the enrollment of the biometric trait into the system. It is not necessary to perform this process onboard; it is too dangerous because there is not enough time to perform enrollment onboard and it is safer to know that the authorized personnel will already have their biometric stored in the database and securely written to the trusted DVD.

Both designs contain distributed enrollment facilities. Security mechanisms should be set forth in order to have policies and procedures at these distributed facilities. For example, every facility must ensure that they contain the same information as the other facilities do. Every enrollment facility must have the same biometric template database as the other enrollment facilities. The matching facilities will also have up-to-date database information (i.e. accurate as to when new users are added/deleted from the database) and will contain the same information as the enrollment facilities except that the matching facilities are used (only) to match live templates with previously stored templates for Design #1, and only in the event of an emergency for Design #2.

A strict security policy should be set in place for enrollment facilities as well. The personnel at the enrollment facilities are responsible for checking the identification of the users who wish to enroll their biometric traits into the large database. This physical identification scheme adds an extra layer of security because we will be aware that whoever has enrolled into the system is actually authorized to be there.

C. FLIGHT DECK PROCEDURES AND BIOMETRIC AUTHENTICATION

In order to maintain efficiency pilots, co-pilots, and other authorized aircraft personnel must follow certain procedures every time they go to work. The flight deck is a complex system in itself and it takes skilled and alert personnel to operate all of the buttons and switches that are located therein. As stated in [8], in complex human-machine systems such as the flight deck, successful operations depend on an elaborate set of procedures. These procedures are the tasks performed by the pilot and/or co-pilot. In order to perform the required tasks, the authorized personnel must be able to follow a well-defined set of rules and guidelines, which are clearly defined in the documents that are located there. If there are checklists provided for the crew, everything will be completed with no problems as long as the checklist is followed in the intended manner.

In the case of the flight deck, there exists a set of standard operating procedures (SOPs) [8]. These procedures provide the crew with a step-by-step guidance for carrying out certain operations. It is important to be able to understand what aircraft personnel are doing prior, during, and after a flight segment so that deployment of a biometric system for continuous authentication will not interfere with their procedural obligations. It is equally important that such a biometric system in the flight deck does not overwhelm aircraft personnel with biometric obligations forcing them to ignore their normal procedures or fail to properly make use of the biometric authentication device.

Standardization of procedures for operations in the flight deck is a critical aspect of flight operations because crewmembers are paired up for each trip without consideration of whether they know each other; paring operations are done remotely, and no direct management supervision is maintained [8]. It must be ensured that the procedures for using continuous biometric authentication in the flight deck are well designed such that there is no confusion as to how those procedures are supposed to be performed. The procedures must be straightforward because a procedure that is ponderous and is perceived as increasing workload, and/or interrupting the smooth flow of flight deck tasks will probably be ignored [8]. Ignoring the task of authenticating using the biometric system in the flight deck should never become an issue.

Many flight deck procedures are dependant on the activities of exterior agents such as air traffic controllers. This idea is analogous to the procedures that must be followed in order to correctly conduct biometric authentication in the flight deck because not only do the aircraft personnel have to authenticate themselves but it is possible that someone on the ground is waiting for authentication data to be transmitted. This idea is the same for the authenticating subject (i.e. the aircraft personnel using the biometric device) because they have to depend and wait for the biometric system to respond. That is why communication between the biometric device in the flight deck and the external agent (i.e. the trusted computer operator on the receiving end) needs to be clear and concise. It is equally important that the communication information be transmitted in a secure and reliable way.

There are two factors, which affect the flow of procedures in the flight deck [8]:

- The sequencing of tasks and procedures and
- Actual scheduling of tasks and procedures

The designer of the SOPs and checklists specifies the sequencing of tasks and procedures and the actual scheduling of tasks and procedures is conducted by the flight deck crew [8, 9]. Since these two factors affect the flow of procedures currently being conducted in the flight deck, the sequencing and scheduling of the procedures for biometric authentication in the flight deck must leave current tasks and procedures undisturbed. Procedures for biometric authentication should be compatible with the biometric technology being deployed as well as with existing flight deck procedures.

Checklists for airline personnel ensure the safety of the flight. It is important that the authorized personnel follow checklists precisely. The checklist procedure is supposed to verify that the plane is configured correctly [9] but some people argue that there is no guarantee of absolute safety simply by completing the tasks that are on the checklist. This argument pertains to long and detailed checklists, which may pose a problem in the event that a pilot may choose not to use the checklist or may conduct the procedure poorly because of its length [8]. If an adequate biometric system were to be employed in the flight deck it is possible that some tasks regarding the biometric system may be incorporated into existing checklists. It is also possible that a separate checklist may be provided which would only pertain to the biometric system at hand. Incorporating items into an existing checklist may pose a problem especially if the existing checklist is already long and tedious.

If there were a biometric device to allow entrance to the flight deck integrated with a continuous biometric authentication system inside of the flight deck, threats may be minimized or the outcome different. If the operator of the computer that is collecting the biometric information notices a problem, then the appropriate people can take some action in regard to the aircraft at risk. The actions that are taken on an aircraft whose biometric authentication system sends a warning to the operator who is looking at the biometric data that is being sent is beyond the scope of this study. It is important to point out that there are various scenarios for dealing with such situations. There are measures to counter a possible take-over of an aircraft but these will not be discussed any further in this study.

Certain concerns focus on the transmission of the biometric data. There may be secrecy concerns coming from the subject who is using the biometric system. Some of the people who may be concerned about privacy issues range from the pilots to their unions (Air Line Pilots Association) as well as many others who may be involved with the specific biometric system. This study will focus on the secrecy and integrity of the data being sent (i.e. biometric data) but not on any specific privacy concerns that may come about by using the biometric system.

Federal Aviation Regulation 121.385 paragraph c states that the minimum pilot crew is two pilots and the certificate holder shall designate one pilot as pilot in command and the other second in command. Since there will always be at least 2 crew members inside of the flight deck, the biometric system must be applicable to all authorized aircraft personnel within the aircraft and not restricted to only one crewmember (i.e. the pilot). This is important because there may be an emergency situation where the co-pilot may have to take over a flight and this type of event should not result in alarms from the biometric system.

In order to accurately and correctly design a checklist for the biometric device in the flight deck; a set of guidelines would be good to have as a reference point for the designers of the system. A set of guidelines for checklist design and usage is given by Degani and Wiener [31]. They observed 42 flight crews so that they would be able to gain an insight into the process, techniques, and the potential problems that are associated with checklist usage in an operational setting.

1. Recommended Practices and Guidelines for Flight Deck Design

As explained in [12], there are some recommended practices that need to be followed prior and during the integration of devices within the flight deck. [12] is consistent with the newly developed FAA and Industry guide to Product Certification, published in Jan. 1999. The sections of [12] cover every step in introducing new devices to the flight deck. Topics related to this study include: Independence & Interaction, Training Requirements, Anthropometric Considerations, Complexity/Automation, and Flight deck lighting [12].

Independence & Interaction is an important consideration when introducing a new device to the flight deck. An independent, stand-alone system that does not interact with other aspects of the pilot interface in the flight deck would most likely require little analysis or evaluation. However, for components that are more integrated with other systems in the flight deck and/or with higher levels of interaction and that perform functions critical to safe flight, more in-depth evaluations with greater fidelity will need to be conducted. The flight deck biometric authentication system could be stand-alone, independent of other cockpit devices.

Training Requirements for new devices introduced to the flight deck should be clearly defined. Products that are relatively simple to learn and operate in the flight deck would most likely require little analysis or evaluation [12].

The analysis and evaluation of the flight deck biometric authentication system would be carried out prior to actual deployment. In [12], it is mentioned that the goal is to make the system as simple to use as possible so that little or no training is required. A flight deck biometric authentication system may require user training to ensure its correct use. It would be nearly impossible to deploy a system and not expect its users to be fully trained and familiar with the system. This idea is analogous to deploying a new “office suite” package; upper management and whoever else uses the application ideally would be properly trained prior to usage.

Some anthropometrical considerations are the comfortable use and accessible placement of the biometric device in the flight deck. To correctly use the flight deck biometric authentication system, it needs to be readily accessible by the pilot and co-pilot. Current controls and displays in the flight deck are in easy reach of both the pilot and co-pilot. As mentioned in [12], all equipment should be operable from the normal pilot's station without removal of the safety belt or other equipment.

Since the biometric system is intended to provide continuous authentication, it should be in a convenient place. This convenience should not weaken security in the sense that a potential attacker or terrorist may be able to use or disable the device. Since it is not possible to conceal the location of the biometric device onboard the aircraft, there should be strong physical security.

Complex manual and automated systems impose demands on the pilot that are difficult to envision and understand [12]. The integration of a flight deck biometric authentication system should not introduce new problems that would prevent the pilot or co-pilot from using the device. The pilot and co-pilot have many duties that they need to take care of prior to flight, during flight, and after the flight so the biometric authentication system that is integrated in the flight deck should not demand difficult or impossible tasks from the pilot or co-pilot.

The biometric system should be tested in a realistic setting prior to deployment. If the biometric authentication system is tested in a realistic setting, such as in a place that resembles an actual flight deck, then we will get an idea as to how the system will perform in that setting. Testing the authentication system in this setting will allow the integrators alleviate the problems that may exist in the flight deck prior to actual implementation.

The lighting conditions in the flight deck do not stay uniform throughout a flight segment. All controls should be easy to locate and read under all ambient lighting conditions in the flight deck [12]. The same is true for the integrated biometric system. The pilot or co-pilot should be able to accurately use the system under any type of lighting conditions. Some methods of biometrics are sensitive to lighting conditions (i.e. retinal scanning), so this must be taken into consideration in selecting a biometric authentication system.

2. Guidelines for Checklist Design and Usage

A good guideline is needed for the design and use of checklists. The flight crew depends on these checklists and procedures in order to correctly report preparedness and readiness prior, during, and after a flight segment. I will present only those guidelines for checklist design and usage that pertain to designing and using a checklist for the flight deck biometric authentication system. The following guidelines only represent a subset of the guidelines introduced in [12].

- Checklist responses should portray the desired status or the value of the item being considered not just “checked” or “set”. This is true for the biometric system because we don’t want to know if the system is just powered on; we at least want to know if the system is working correctly and is ready to do its designated job. This is especially true for the secure channel check to ensure the data that is transmitted to its designated source for template comparison. It must be ensured that the secure channel is up and ready.
- The use of hands and fingers to touch, or point to, appropriate controls, switches, and displays while conducting the checklist is recommended. This may be done with a quick test done by the appropriate personnel (i.e. a quick touch of the fingerprint scanner or a quick sound of the voice over a voice scanning device).
- Sequencing of checklist items should follow the “geographical” organization of the items in the flight deck, and be performed in a logical flow. Somewhere in the existing checklist there will be an entry that pertains to the biometric system. This entry should depend on where the biometric system is placed in the flight deck (e.g. there may be a voice authentication device at or around the microphone area and a thumbprint reader by the seat of the pilot).
- Checklists should be designed so that their execution will not be tightly coupled with other tasks. As with any other task done prior, during, and

after a flight, the biometric system checklist should have equal importantance. It would be up to the discretion of the implementers of the biometric system checklist to ensure that this task does not interrupt existing tasks at hand.

This small set of guidelines provides a starting point for designing a checklist for the flight deck biometric authentication system.

3. Policies and Procedures

In general, policies are broad specifications of the manner in which management expects things to be done. In the airline industry this concept applies to training, flying, and maintenance. Policies would have to be defined for training of the flight crew to correctly use the flight deck biometric authentication system, using the biometric system while in flight, and maintenance. Procedures for the biometric authentication system onboard the aircraft should be designed to be as consistent as possible with the policies already defined for the flight deck. Furthermore, there shouldn't be a procedure that would limit the biometric authentication to one flight crewmember because there may be a policy defined for the dynamic use of that biometric system. The procedures and policies should not contradict each other and should be defined in parallel (if possible).

Procedures exist in order to specify, unambiguously, six things [10]:

- What the task is. In terms of the flight deck biometric authentication system, this may simply explain what initially needs to be done with the system to prepare it for usage or what the steps to take would be if an error message were to appear on the screen.
- When the task is conducted. Initial startup for the biometric system must be done prior to flight and authentication must be done during flight, for example.
- Defining who conducts the task. It is possible that the main pilot is responsible for some of the tasks associated with the biometric system and the co-pilot may be responsible for a separate task regarding the same

biometric system. This is where communication between the pilot and co-pilot is crucial.

- How the task is done. Specifying exactly what needs to be done will eliminate confusion or simple human error. For example, there may be a document that explains how to bring up a certain application in the biometric system that may be needed during flight.
- What the sequence of actions consists of. This may apply to a specific biometric device (e.g. if there was a fingerprint scanning device in the flight deck, then there may be a refresher set of instructions on how to use the device).
- What type of feedback is provided. This may apply to the acceptance or rejection of the user when they are using the biometric device or system (e.g. an accepted message relayed back to the user).

Introducing any new technology, a biometric system in this case, into the flight deck or any other domain requires the procedure designer to [12]:

- Reevaluate all of the existing concepts and policies in light of the new technology
- Support the new technology via new procedures

The integration of a biometric authentication device onboard the aircraft is a big change and quick adaptation is the desired outcome. The procedure designer, in this case, would need to reevaluate all of the existing concepts and policies in light of the new biometric authentication system and support this system by implementing a new set of procedures. This change needs to have a clear definition for everyone involved to understand, especially the procedure designer. Manuals, documents, checklists, and many other paper forms are already used in the flight deck. Along with the existing documents there will be documents, manuals, and checklists that pertain to the flight deck biometric authentication system. All of these related documents and paper forms must be kept in convenient, easy to locate areas. Fast retrieval of these important documents must be possible in the event of a system breakdown or abnormalities with the system.

Since the biometric system would apply to all of the authorized aircraft personnel, it is important to be able to maintain coordination and communication within the flight crew and with any relevant external agents. Coordination and communication applies to any action from start-up of the system to its shutdown (if applicable) and any other action in-between.

Procedures should be clear and explicit, not too vague. Vagueness violates one of the most important by-products of flight deck procedures: coordination of tasks between agents [10]. If the procedures for the biometric system are straightforward and comprehensible then there should be no problems in following them. Moreover, the biometric system's procedures should not yield different outcomes for the same task (e.g. when the biometric system task list calls for starting up the system, only one outcome will come about, the system will be powered up).

Policies help to guide users into a frame of mind that will aid them in distinguishing between right and wrong in terms of what management wants them to do. For example, a college computer laboratory may have policies set in place that prohibit the downloading of music while users are logged into their systems (in the lab or through dial-up). Management or, in this case, the school's system administrator may view these policies differently than students. Similarly different interpretations of policy may be held by different members of the airline industry. Policies should take into account the operation and security of the biometric system and the security of the documents associated with the biometric system. Setting final policies in regard to the biometric system employed in the flight deck is beyond the scope of this study.

D. SECURITY CONSIDERATIONS FOR FLIGHT DECK BIOMETRICS

In order to implement biometrics in the flight deck, one must take into consideration the security requirements that such a system should or must meet prior to implementation. If security policies are put in place and are abided to by the users, then the system is less vulnerable to many known attacks or the degrading of services or systems. This

At the enrollment facilities, it should be a part of the security policy to physically check the identification of users who are attempting to enroll (i.e. having two forms of identification as a requirement, for example). By having this physical checking of identification, we are reducing the chances of an unauthorized person enrolling into the system. We will know who is enrolling their biometric data into the system with high assurance. The actual enrollment room, where the biometric device resides, should be physically secure as well. Physical security of this area is possible by inserting padlocks or cipher locks on the doors in order to control access. As users complete their enrollment process, the authorized person, who is in charge of overseeing the whole process, should also keep pen and paper logs of who has enrolled into the system for a given day, if possible. These pen and paper logs can be compared to an electronic counting device, which can be used to keep a numerical value of how many users have enrolled for a given day, this can be used for added security.

Since the enrollment facilities are responsible for communicating all information to the matching facilities, this communication is secure. If the enrollment facilities are responsible for providing trusted DVDs to the matching facilities and the trusted PC onboard the aircraft, then this must also be done in a highly secure manner. If the biometric template database is saved onto a DVD, as in Design #2, these DVDs must be of high integrity to begin with. Since the biometric template database may change often (i.e. additions, deletions), it is important that the updated information be put on DVDs and distributed to the appropriate locations in a timely manner.

The matching facilities have the same responsibilities in both of the design proposals. One difference is in Design #1, where the matching facilities have to relay a message back to the flight deck. This message is basically the outcome given from the biometric device (i.e. acceptance or rejection). The distributed matching facilities will each have a copy of the biometric template database. This information must be protected and should not be vulnerable to known attacks. If the biometric template database is on DVDs, those DVDs need to be kept in a secure place so they are not liable to theft or manipulation. The DVDs can also be encrypted to prevent manipulation or extraction of information (the movie industry supports this to prevent movie piracy).

The biometric device(s) should be protected from tampering and theft. These device(s) in the flight deck should only be accessed and used by authorized personnel. The biometric device(s) used at the enrollment facilities should also be protected from tampering and theft. These devices at the enrollment facilities can be physically secured, in a separate room, along with the other devices used for enrollment purposes. One way in which the biometric device(s) can be secured in the flight deck is to provide an access control mechanism into the flight deck (i.e. implementing a biometric device outside of the flight deck region such that only authorized personnel are allowed into this area). Another way that the biometric device(s) can be secured in the flight deck is to provide the location of the device(s) on a need to know basis. For example, passengers do not need to know where the devices are stored and used, but the co-pilot or flight attendant has to know where these devices are. The use of a biometric device or system of devices in the flight deck can be done very discretely, with no effect on any other persons onboard.

Strengthening the security policies for the biometric system will aid in protecting the system throughout its lifetime and use. Education pertaining to the security policies for the users of the system is necessary so that they fully understand and abide by them. Training eliminates simple mistakes by the user and can be done either during enrollment or separately, depending on how the system is set up and whether a single biometric or several biometric methods will be used. Training can be analogous to the training that the pilots received in order to carry a gun onboard the aircraft, but not as intensive.

E. ANCILLARY CONSIDERATIONS

1. Biometric Template Size and Processing Time

Depending on how many templates need to be stored in this database, the template size of various biometrics may become an issue. Some approximate biometric template sizes are [30]:

• Voice	70 – 80Bytes/second
• Face	84 – 2000 B
• Fingerprint	256 B – 1200 B
• Hand Geometry	9B
• Iris	256 B – 512 B
• Retina	96B

Template sizes vary for every biometric method. If a biometric method is chosen with a higher approximate template size, then it may be possible to store these templates in a compressed form within its storage device. If the biometric templates are stored in a trusted DVD, as proposed in Design #2, then compression may not be needed since DVDs can hold 4.7 GB of data on each side (if the DVD is double sided).

The processing time needed to perform matching of a live template to a stored template and from when the user enrolls his/her biometric to the time that the enrolled biometric is converted into its numerical equivalent needs to be as close to real time as possible. Processing speed for computer systems continues to grow rapidly so it should not be a problem in choosing an appropriate system for this purpose. Lastly, clear and concise templates are necessary for storage and accurate matching later on in the process.

2. Enrollment Facilities System

The system for the enrollment facilities has to be physically secured. This system should possess the capability that would allow an authorized user to add and delete templates as needed. Deleted templates need to be taken off the system permanently and there should be a mechanism available to validate that this has been done correctly. The system should not allow the recovery of deleted items (i.e. templates) and the accuracy of data collection is a must.

A system security policy needs to be set in place that covers audit trail information, quality control, system management, and assurance level. Audit trail information should include the time of the event, event type, and the outcome of the event (i.e. rejection or acceptance of the user into the system). System management may include the enforcement of security policies. The assurance level of the system should be high at all times and the integrity of the system should not be, or become, vulnerable to attack. If this system is vulnerable to attack, a lot of vital information can be compromised. This vital information could be the actual biometric templates that are stored in the system or the password to get into the system.

Backups are an important aspect of system administration and should be equally important for the biometric authentication system as well. A good backup system will always be useful in the event of a system breakdown. If backups are created regularly, they will contain the most up to date information. Not only do we need backups of biometric templates, we also need a backup of the entire system in the event that something happens to the main biometric authentication system. For example, if the main system crashes or freezes, there would be no way to be able to recover the lost data without having an adequate backup system. Furthermore, if the system is in an unstable state when it freezes up then there may be some loss of data; this is where the backup system comes in handy since it contains the same information as the main system does. The level of redundancy and fault tolerance needed is out of the scope of this study.

3. Trusted PC Onboard the Aircraft

The trusted PC onboard the aircraft should be non-bypassable, tamperproof, and physically secure. The onboard PCs main responsibility is the matching of live templates against stored templates and either accepting or rejecting the user based on his or her score in relation to the initial threshold. There should not be a delete/add users mechanism on this particular PC because it is only used for matching purposes and providing outcome to the users or situation assessment personnel.

Just like the PC used at the enrollment site, this PC should also have a system security policy, which would cover the same aspects and ideas as the enrollment site PCs. The onboard biometric system, including the trusted matching device is a stand-alone system and should not depend on other devices in the flight deck of the aircraft.

4. Summary

Based upon technical considerations and high-level requirements two designs have been proposed for continuous in-flight authentication of personnel on the flight deck. The next chapter will provide conclusions for this study and possible avenues for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

As evidenced by recent world events, there is a need to increase security onboard commercial aircraft. Many current measures seek security fortifications outside of the flight deck. For example, our airports contain many more security screeners and many other security provisions have been set in place, including the arming of some pilots in the flight deck. Positive identification of personnel in the flight deck is needed. By using biometrics in the flight deck, we can solve the authentication problem in the flight deck and for this; two designs are presented.

Many biometric methods are introduced in this study, from fingerprint to facial recognition, but there are many newer biometric methods that have not been included due to lack of sufficient data regarding their effectiveness. As single biometric devices may suffice for authentication in the flight deck, so might the use of multi-biometrics improve an authentication system in the flight deck. More studies in multi-biometrics are needed in order for the effectiveness to be understood.

How can we implement a secure biometric authentication system onboard an aircraft? Proposed Designs #1 and #2 serve to answer this question. Proposed Design #1 takes advantage of the idea of secured communication channels, where biometric templates must travel back and forth from the flight deck to the matching facilities whereas proposed Design #2 eliminates the need for secured communication channels external to the aircraft. Proposed Design #2 takes advantage of the idea of mass storage (i.e. the database full of authorized user's templates) stored on reasonably small media (i.e. DVDs) and having a trusted PC onboard the aircraft.

Prior to choosing an adequate biometric method, one needs to carefully research biometric performance measurements. These measurements are important when we are balancing security and convenience. Biometric vulnerabilities are defined so that they can be mitigated before clever attackers use them. This document serves to introduce and define security considerations for the use of biometric authentication in the flight deck. A means of protecting data by providing procedures that allow you to automatically recover from hardware failures (fault tolerance) in terms of critical user data (their biometric information) and system reliability are topics for future research.

Further research for use of biometric systems in the flight deck should be done in the area of multi-biometrics. If additional research and testing (on combining different biometric methods together) is done in this area, we would then have sufficient information that would be useful in choosing the best biometric methods to combine together to form a strong system overall.

This thesis has examined the problem of authentication in the flight deck. Several biometric techniques were reviewed, flight deck requirements were given, and two designs were developed and discussed. Expansion of the designs proposed herein is possible to accommodate advances in the area biometric technology and biometric authentication systems. Future developments in biometric technology should make one of these designs feasible and highly reliable.

LIST OF REFERENCES

[1] An MIT Enterprise Technology Review, Paper, November 2001.

[2] Anderson, E.A., “A Demonstration of the Subversion Threat: Facing a Critical Responsibility in the Defense of Cyberspace”. Master’s Thesis, Department of Computer Science, 2002, Naval Postgraduate School, Monterey, CA.

[3] Bruderlin R. “What is biometrics?” Paper, 1999-2001.

[4] Bonsor K. “How Facial Recognition Systems Work”, 2001.

[5] Chua J. Biometrics, “The future of security”, CBC News Online, September 2001.

[6] Daugman J. “Combining Multiple Biometrics”, the Computer Laboratory at Cambridge University, 2000.

[7] Daugman J. How iris recognition works, 2000.

[8] Degami A., Wiener E.L. Procedures in Complex Systems: The Airline Cockpit, NASA contractor report 177642, Moffett Field, CA: NASA Ames Research Center, 1997.

[9] Degami A, Weiner E.L. Cockpit Checklists: Concepts, Design, and Use, NASA contractor report 177549, Moffett Field, CA: NASA Ames Research Center, 1993.

[10] Degami A. On the Design of Flight Deck Procedures, NASA contractor report 177642, Moffett Field, CA: NASA Ames Research Center, 1994.

[11] Esser M. “Biometric Authentication”, Essay, October 2000.

[12] General Aviation Manufactures Assoication, Recommended Practices and Guidelines for Part 23 Cockpit/Flight Deck Design GAMA Publication No. 10 September 2000.

[13] Go Team 9- Biometrics, U.S Department of Transportation; Transportation Security Administration Technical Report.

[14] Govindarajan S. Are These Prying Eyes, article, available
http://www.krify.com/articles/pryingeyes.htm (last accessed: November 2002)

[15] Hong L. and Jain A.K. Integrating Faces and Fingerprints, IEEE Trans. Pattern Anal. Machine Intell., Vol. 20, No. 12, pp. 1295-1307, December 1998.

[16] Info Security Magazine, “Biometrics Technology: Making Moves in the Security Game", pp. 28-34 Volume 12 #3 March 2002.

[17] International Biometrics Group, Tech Reports “Facial Scan Technology: How it works”, 2002.

[18] International Biometrics Group, Tech Reports “Iris-Scan: How it works”, 2002.

[19] Jain A.K and Arun R. Learning user-specific parameters in a multibiometric system, Department of Computer Science and Engineering-Michigan State University, no date given.

[20] Kolettis H. Stepping up Security, 2002.

[21] Liu S. and Silverman M. A practical guide to biometric security technology, January 2000.

[22] National Center for State Courts, “Hand Geometry”, no date given.

[23] Mansfield T., Kelly G., Chandler D., Kane J., Biometric product testing final report CESG contract X92A/4009309 Issue 1.0, March 2001.

[24] Mansfield A.J and Wayman J.L. Best Practices in Testing and Reporting Performance of Biometric Devices, August 2002.

[25] Prabhakar J. and Pankanti “On the Individuality of Fingerprints”, 2001.

[26] Putte T. and Keuing J. “Biometrical Fingerprint Recognition Don’t Get Your Fingers Burned”, Paper, September 2001.

[27] Schneier, B. “Fun with Fingerprint Readers”, Crypto-Gram Newsletter, May 15, 2002.

[28] Sperry P. “Captains to FAA: Focus on Cockpits”, 2001, article, available http://www.rightswatch.org/safer_skies/focus_cocpits.htm (last accessed: January 2003)

[29] UK Biometrics Working Group, Use of biometrics for identification and authentication: Advice on product selection, November 2001.

[30] Woodward J.D, Orlans N.M, Higgins P.T. Biometrics Identity Assurance in the Information Age (2003).

[31] Zhang D. Biometric Solutions for Authentication in an E-world, November 1, 2002.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Dr. Ernest McDuffie
   National Science Foundation
   Arlington, VA

4. RADM Zelebor
   N6/Deputy DON CIO
   Arlington, VA

5. Russell Jones
   N641
   Arlington, VA

6. David Wirth
   N641
   Arlington, VA

7. CAPT Sheila McCoy
   Headquarters U.S. Navy
   Arlington, VA

8. CAPT Robert Zellmann
   CNO Staff N614
   Arlington, VA

9. Dr. Ralph Wachter
   ONR
   Arlington, VA

10. Dr. Frank Deckelman
    ONR
    Arlington, VA

11. Richard Hale
    DISA
    Falls Church, VA

12. George Bieber
OSD
Washington, DC

13. Deborah Cooper
DC Associates, LLC
Roslyn, VA

14. David Ladd
Microsoft Corporation
Redmond, WA

15. Marshall Potter
Federal Aviation Administration
Washington, DC

16. Ernest Lucier
Federal Aviation Administration
Washington, DC

17. Keith Schwalm
DHS
Washington, DC

18. RADM Joseph Burns
Fort George Meade, MD

19. Howard Andrews
CFFC
Norfolk, VA

20. Steve LaFountain
NSA
Fort Meade, MD

21. Penny Lehtola
NSA
Fort Meade, MD

22. Dr. Shaun Cooper
New Mexico State University
Las Cruces, NM

23. Mary H. Carrillo
Department of Public Safety
Santa Fe, NM

24. Dr. Cynthia Irvine
Naval Postgraduate School
Monterey, CA

25. Timothy Levin
Naval Postgraduate School
Monterey, CA

26. Cassandra Carrillo
Naval Postgraduate School
Monterey, CA